● 国家出版基金资助项目

中国科学院华罗庚数学重点实验室丛书

# 华罗庚文集

## 数论卷 III

王元 潘承彪 贾朝华 / 编译

科学出版社
www.sciencep.com

中国科学院华罗庚数学重点实验室丛书

华罗庚文集 | 数论卷 III |




销售分类建议：高等数学

定 价：98.00元

国家出版基金资助项目

中国科学院华罗庚数学重点实验室丛书

# 华罗庚文集

## 数论卷 III

王 元 潘承彪 贾朝华 编译

科 学 出 版 社
北 京

## 内 容 简 介

本书精选、翻译了华罗庚在各个时期数论方面的代表性论文，这些论文是关于华林问题、Tarry 问题、指数和估计、Vinogradov 中值定理、整数分拆、Pell 方程的最小解、最小原根、圆内格点等重要数论问题的研究.

本书适合数学专业的大学生、研究生、教师、科研工作者以及对华罗庚学术思想有兴趣的读者阅读.


图书在版编目(CIP)数据

华罗庚文集：数论卷Ⅲ/王元，潘承彪，贾朝华编译. —北京：科学出版社，2010

(中国科学院华罗庚数学重点实验室丛书)

ISBN 978-7-03-028514-0

Ⅰ.华… Ⅱ.①王… ②潘… ③贾… Ⅲ.①数学-文集 ②数论-文集 Ⅳ.O1-53

中国版本图书馆 CIP 数据核字(2010)第 151898 号

责任编辑：张 扬 赵彦超 / 责任校对：陈玉凤
责任印制：钱玉芬 / 封面设计：陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

中国科学院印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2010 年 8 月第 一 版 开本：B5(720×1000)
2010 年 8 月第一次印刷 印张：20 3/4
印数：1—3 000 字数：404 000

定价：98.00 元

(如有印装质量问题，我社负责调换)

# 《华罗庚文集》序言

2010 年是著名数学家华罗庚先生诞辰 100 周年. 值此机会, 我们编辑出版《华罗庚文集》, 作为对他的美好纪念.

华罗庚先生是他那个时代的国际领袖数学家之一, 也是中国现代数学的主要奠基人和领导者. 无论是在和平建设时期, 还是在政治动荡甚至是战争年代, 他都抱定了为国家和人民服务的宗旨, 为中国数学的发展倾注了毕生精力, 受到了中国人民的广泛尊敬.

华罗庚先生最初研究数论, 后将研究兴趣拓展至代数和多复变等多个领域, 取得了一系列国际一流的成果, 引领了这些领域的学术发展, 产生了广泛持久的影响. 他从一名自学青年成长为著名数学家, 其传奇经历激励了几代中国数学家投身于数学事业.

华罗庚先生为我们留下了丰富的精神遗产, 包括大量的学术著作和研究论文. 我们认为, 认真研读这些著作和论文, 是深刻把握华罗庚学术思想精髓的最佳途径. 无论对于数学工作者还是青年学生, 其中许多内容都是很有启发和裨益的.

华罗庚先生担任中国科学院数学研究所所长 30 余年, 他言传身教, 培养和影响了一批国际水平的数学家, 他的学术思想和治学精神已经成为数学所文化的核心. 自 2008 年起以中科院数学所为基础成立的中国科学院华罗庚数学重点实验室, 旨在继承和弘扬华罗庚先生的学术思想和治学精神, 积极推动中国数学的发展. 为此, 我们选择华罗庚先生的著作和论文作为实验室的首批出版物, 今后还将陆续推出更多优秀的数学出版物.

在出版《华罗庚文集》的过程中, 我们得到了各方面的关心和支持, 包括国家出版基金的资助, 在此我们表示深深的感谢. 同时, 对于有关人员在策划、翻译和审校等方面付出的辛勤劳动, 对于科学出版社所作的大量工作, 我们表示诚挚的谢意.

中国科学院华罗庚数学重点实验室

《华罗庚文集》编委会

2010 年 3 月

# 目　　录

# 华罗庚 (1910–1985)[①]

哈贝斯坦　著

王　元　译

**哈贝斯坦教授曾任美国伊利诺伊大学数学系主任, 研究方向是解析数论, 现已退休. 华罗庚教授曾在 1948 —1950 年间任伊利诺伊大学的教授, 回国之后与哈贝斯坦的友谊保持终生. 哈贝斯坦教授的这篇有关著名数学家华罗庚的传记文章, 发表在美国科学院出版的《科学家传记》第 81 卷 (*Biographical Memoirs*, Vol.81. Washington, D. C.: The National Academy Press, 2002) 中. 该传记丛书每卷大约 500 页, 包括 20 名科学家. 据查, 在 70—81 卷中, 只收录了一位大陆科学家 —— 华罗庚. 本传记中的观点均属于作者本人, 并不一定反映美国国家科学院的观点.**

华罗庚是他那个时代的领袖数学家之一及他那一代人中两位最杰出的中国数学家之一, 另一位是陈省身. 正当中国在经历一场又一场政治波动的时候, 华罗庚度过了年富力强的年代. 如果今天许多中国数学家能在科学前沿作出突出的贡献, 如果数学在中国享有异常的普遍尊重, 那就要在很大程度上归功于作为学者与教师的华罗庚 50 年来对他国家的数学事业的领导.

华罗庚于 1910 年生于中国江苏省南部的金坛县. 现在金坛已经是一个繁荣的城市, 它有一所以华罗庚命名的中学及一个颂扬他功绩的纪念馆. 但在 1910 年, 金坛还只是一个小村镇, 华罗庚的父亲在那里开一家杂货店. 在华罗庚的整个青少年时期, 他的家庭都是很贫穷的. 除此之外, 他还是一个不断被病痛折磨的羸弱孩子, 在一次伤寒病后竟使左腿瘫痪了, 这给他带来终生行走时的严重不便. 但很幸运地, 华罗庚天性愉快与乐观, 这对他以后遇到困难时是很有帮助的.

华罗庚受到的正规教育是短暂的, 从表面上看, 它几乎不足以奠定学术生涯的基础 —— 他得到的第一个学位为 1980 年法国南锡 (Nancy) 大学授予的荣誉博士, 然而, 优质的正规教育使他得到了智力的发展. 1922 年, 当华罗庚小学毕业时, 金坛中学开办了, 该校有一位高素质与严格的数学老师, 他认识到华罗庚的才能并加以培养. 此外, 华罗庚在很早就养成了缺少书籍时自学的习惯, 往后, 在缺少文献的情况下, 直接去处理问题成为他的首要原则, 在他的一生中都热情地贯穿这一原则,

① 本文原载《中国科技史料》第 23 卷, 第 3 期 (2002 年): 181–188.

并鼓励他的学生也用这一方法.

其后, 华罗庚进入了位于上海的中华职业学校, 在那里, 他荣获过全市珠算比赛冠军. 尽管学校的学费较低, 但生活费用对华罗庚来说还是太高了, 从而迫使他在差一学期就要毕业时便辍学了. 华罗庚无法在上海找到一份工作, 只好在 1927 年回老家帮助他的父亲经营杂货店. 同年, 他与吴筱元结婚, 次年得女儿华顺, 1931 年又得长子华俊东.

华罗庚回到金坛后, 即开始自学数学并在上海《科学》杂志 1929 年 12 月号上发表了他的处女作《Sturm 氏定理的研究》. 次年, 在同一杂志上发表的一篇短文中, 华罗庚指出了该杂志在 1926 年发表的五次方程可解的文章有原则性错误. 华罗庚透澈的分析得到了北京清华大学一位伯乐教授的青睐. 尽管他缺乏正式学历并有部分教员持保留意见, 华罗庚仍于 1931 年被邀请到该校数学系工作, 开始时任图书馆管理员, 然后改任数学助教; 1932 年 9 月他开始授微积分课; 两年后晋升为教员, 那时, 华罗庚已发表了十多篇文章, 从其中一些文章中, 人们可以看出他将来的兴趣所在. 由于他的才华与贡献, 24 岁的华罗庚已经是一位职业数学家了.

这时的清华大学是中国高等教育的最高学府, 那里的教员致力于使中国的数学与科学赶上西方的先进水平. 中国的科学在停滞了数百年之后, 这无疑是一项极艰难的工作. 在 1935 年和 1936 年, 阿达马 (J. S. Hadamard) 与维纳 (Norbert Wiener) 访问了清华大学, 华罗庚热切地听了他们二人的讲课并给他们留下了良好的印象. 随后维纳访问了英国并向哈代 (G. H. Hardy) 介绍了华罗庚, 从而, 华罗庚得到了英国剑桥大学的邀请. 他于 1936 年到达剑桥. 在那里, 他度过了富于成果的两年. 在华林 (Waring) 问题范围内的众多方面, 华罗庚发表了不少论文 (还有丢番图分析与函数论的一些课题). 华罗庚很好地利用了声誉达到顶点的哈代–李特尔伍德 (J. E. Littlewood) 学派的学术环境, 华罗庚是靠中华文化教育基金会每年 1250 美元的资助在英国生活的. 我们饶有兴趣地回顾一下, 该基金来自于中国在 19 世纪与美国及其他一些国家在中国进行的战争对美国的赔款中退回来的钱 (译者注: 即 "八国联军" 入侵, 在屈辱的《辛丑条约》中规定的赔款 ——"庚子赔款"), 这一赔款是强权强加于中国的. 哈代向华罗庚保证, 在两年中他便能轻易地得到博士学位, 但是华罗庚因交不起学费而取消了拿博士的做法. 当然, 他对这一决定作了另一个完全不同的解释.

在剑桥期间, 华罗庚成为达文波特 (Harold Davenport) 与海尔布龙 (Hans Heilbronn) 的朋友, 这二人是 "三一学院" 的年轻研究员, 前者为李特尔伍德以前的学生. 而后者为兰道 (E. Landau) 在哥廷根时最后的助教, 华罗庚跟他们一起, 对于哈代–李特尔伍德处理华林问题这类的堆垒问题深感兴趣. 他们帮助修改了华罗庚的一些论文中的英文, 这些论文说明华罗庚是相当高产的. 这一时期华罗庚撰写了超过 10 篇论文, 其中不少篇都发表在伦敦数学会出版的杂志上面.

大概华林问题仅有的简单事情为它的陈述：在 1770 年, 华林断言但未证明以下的命题 (非原话)：对于每一个整数 $k \geqslant 2$, 皆存在一个仅依赖于 $k$ 的整数 $s = s(k)$ 使每一个正整数 $N$ 皆可以表示为

$$N = x_1^k + \cdots + x_s^k, \tag{1}$$

其中 $x_i(i = 1, 2, \cdots, n)$ 为非负整数. 同年, 拉格朗日 (J. L. Lagrange) 证明了 $s(2) = 4$, 即解决了 $k = 2$ 的情况. 这是一个臻于至善的结果; 往后则进展甚缓, 直到 1909 年, 希尔伯特 (D. Hilbert) 才完全解决了一般情况下的华林问题, 他用的方法为复杂的代数恒等式的应用, 而且 $s(k)$ 的值甚大. 1918 年, 哈代与拉马努詹 (S. Ramanujan) 又回到了 $k = 2$ 的情况, 试图用傅里叶 (J. B. J. Fourier) 分析方法决定将整数表为 $s$ 个平方和的表示数目问题. 他们的想法是受到他们关于分拆的著名工作的启发而形成的, 他们成功了, 这就鼓舞了哈代与李特尔伍德在 1920 年将类似的方法用于一般的 $k$. 他们发明了所谓的圆法来处理一般的希尔伯特–华林定理及包括哥德巴赫 (C. Goldbach) 问题在内的一大批堆垒问题. 在往后的 20 年里, 圆法结构的困难程度在整个数学中都被认为是可以与任何其他东西相比拟的. 即使在今天, 在经过众多的改进与很大进展后, 这一方法的复杂性仍然令人望而生畏①. 概要地讲, 经过维诺格拉多夫 (I. M. Vinogradov) 改进过的哈代–李特尔伍德–拉马努詹圆法可以这样来叙述：命

$$T(\alpha) = \sum_{x=0}^{P} \mathrm{e}^{2\pi \mathrm{i} \alpha x^k}, \quad P = [N^{1/k}]$$

及 $R_s^{(k)}$ 表示 $N$ 表为形式 (1) 的表示数, 则

$$R_s^{(k)}(N) = \int_0^1 T(\alpha)^s \mathrm{e}^{-2\pi \mathrm{i} N\alpha} \mathrm{d}\alpha,$$

所以欲证希尔伯特–华林定理, 只要证明当 $s$ 为某个仅依赖于 $k$ 的自然数时, 对于所有充分大的整数 $N$ 皆有 $R_s^{(k)}(N) > 0$ 就够了. 我们记 $G(k)$ 为这种可允许的 $s$ 值中的最小者. 在 [0, 1] 中以较小分母有理数为中心的互不相交的诸小区间的集合上, 生成函数 $T(\alpha)$ 可得到很好的逼近, 从而设想可以证明在这些区间上的积分之和即得到 $R_s^{(k)}(N)$ 的主项, 而关于通常称为劣弧的补集上的积分则为一个较低阶的无穷大. 后面这项工作, 即在劣弧上进行估计, 更为困难些, 但哈代与李特尔伍德在此用了一个比 $T(\alpha)$ 更广泛的三角和的估计, 这是外尔 (Hermann Weyl) 于 1916 年建立的与序列一致分布判别法的基本工作相联系的一项工作. 这样一来, 他们就证

① R. C. Vaughan. *The Hardy-Littlewood Method*, 2nd. Cambridge: Cambridge University Press, 1977.

明了

$$G(k) \leqslant k2^{k-1}+1,$$

这就是华罗庚作为一个青年人的工作背景. 这样说或许是适当的. 华罗庚在这方面的贡献使他青史留名, 即他关于类似于 $T(\alpha)$ 的三角和的单个与平均卓越的原创性估计. 这一种平均估计, 即现在著名的华氏引理是说, 对于任何 $\varepsilon>0$ 及 $1\leqslant j\leqslant k$, 皆有

$$\int_0^1 |T(\alpha)|^{2^j}\mathrm{d}\alpha = 0_\varepsilon(P^{2^j-j+\varepsilon}).$$

显然 $T(\alpha)\leqslant P$, 所以对于每一个 $j\leqslant k$, 这一不等式几乎省去了一个 $P$ 的 $j$ 次方幂. 当在劣弧上与 $T(\alpha)$ 的外尔估计联系使用时, 华氏不等式导出了改进的界

$$G(k)\leqslant 2^k+1.$$

当今虽然有了更好的结果, 但皆为十分困难复杂的.

华罗庚满可以在英国逗留更长的时间, 但他思家心切, 日本于 1937 年入侵了中国, 更使他忧心如焚. 他于 1938 年离开剑桥, 作为一位正教授回到他原来的大学. 这时, 在大部分中国被日本占领后, 清华大学已不在北京了, 它搬到了南方的云南省省会昆明, 与其他几所大学 (指的是北京大学与南开大学 —— 译者注) 一起组成了临时的西南联合大学. 华罗庚与他的家庭一道在昆明一直待到 1945 年第二次世界大战结束. 那时, 华罗庚是很贫穷的, 加上体质很差与学术上的孤立. 尽管困难重重, 华罗庚仍然维持着他在剑桥时的工作强度, 甚至有过之, 至 1945 年底, 他已发表了 70 多篇论文. 在这期间, 他研究了维诺格拉多夫原创性的三角和估计方法并用更精确的形式作了简洁的复述, 即现在普遍熟知的维诺格拉多夫中值定理, 这一著名结果的中心作用为改进希尔伯特–华林定理, 及关于黎曼 (G. F. B. Riemann)$\zeta$-函数研究的重要应用. 华罗庚将这一工作写成一本小册子. 早在 1940 年即被前苏联接受用俄文发表, 但由于战争原因, 直到 1947 年才以斯捷克洛夫 (V. A. Steklov) 数学研究所的专著 (其扩充形式) 正式发表了.

应维诺格拉多夫的邀请, 华罗庚于 1946 年春在俄罗斯呆了 3 个月. 除数学交流外, 华罗庚对那里科学活动的组织甚有好感. 当日后他在新中国处于领导岗位时, 这一经验对他是颇有影响的. 往后的岁月里, 尽管华罗庚的科学活动扩展到了其他领域, 他总是准备回到华林问题及一般数论中来, 特别是回到涉及指数和的问题. 因此在 1959 年, 他发表了为《数学百科全书》(*Enzyklopädie der Matematischen Wissenschaften*) 而写的重要专著《指数和的估计及其在数论中的应用》. 他关于什么东西重要的感知及关于技术的出色掌握使他的数论论文即使在今天来看仍为 20 世纪上半叶数论重要活动的一个索引.

在昆明的后几年中，华罗庚的兴趣转入了代数与分析，首先他着力于使学生得益，继之即在这些领域作出了原创性的贡献. 华罗庚对矩阵代数有兴趣并撰写了一些矩阵几何学方面的实质性论文. 他被邀请访问位于普林斯顿的高等研究院，但由于西格尔 (C. L. Siegel) 在那里做着某些类似的工作，华罗庚起先拒绝了这一邀请，以便能独立地发展他自己的想法. 在华罗庚从俄国回国不久，他仍于 1946 年 9 月启程赴普林斯顿，华罗庚不仅带去了矩阵理论的构想，而且还有多个复变数函数论与群论的计划. 这时中国的内战正酣，因而他难于成行，为此，中国当局在华罗庚的护照上赋予了将军的头衔以 "便于旅行".

按照他的传记作者的看法，华罗庚在美国期间 "最重要与值得的研究工作" 为除环 (skew field) 这一领域，即 (非交换) 可除代数，四元数为除环的一个经典例子. 华罗庚是下面命题的首先证明者，即每一个除环 $F$ 的半自同构或者为一个自同构或者为一个反自同构 —— 更确切地讲，若 $\sigma$ 是一个 $F$ 至自身的一一映射且满足 $1^\sigma = 1$ 及对所有 $F$ 中的 $a, b$ 皆有

$$(a+b)^\sigma = a^\sigma + b^\sigma, \quad (aba)^\sigma = a^\sigma b^\sigma a^\sigma,$$

则对于所有 $a, b \in F$，或者

$$(ab)^\sigma = a^\sigma b^\sigma$$

或者

$$(ab)^\sigma = b^\sigma a^\sigma.$$

他亦给予他 "直接" 处理问题的一个惊人证明，即证明了每一个除环的正规子域必包含在其中心之中，证明只有一页半，它依赖于下面的恒等式：若 $ab \neq ba$，则

$$a = [b^{-1} - (a-1)^{-1}b^{-1}(a-1)][a^{-1}b^{-1}a - (a-1)^{-1}b^{-1}(a-1)].$$

在文献中，这一结果被称为嘉当 (H. Cartan)– 布饶尔 (R. Brauer)– 华氏定理，嘉当最初的证明用到了很多较深奥的工具.

当然，在他生命的最后大创造时期中，他还做了不少别的工作，华罗庚与范迪维尔 (H. Vandiver) 合写了几篇有限域上不定方程求解的文章及与赖纳 (I. Reiner) 合写了典型群自同构的文章. 他的大部分代数工作构成了他在日后与万哲先合写的专著《典型群》(上海科技出版社出版, 1963 年, 中文) 的基础.

在个人方面，1947 年春，华罗庚在约翰 · 霍普金斯大学手术治疗腿疾，经治疗后他的一条瘸腿在行走时有了很大的改善，为此他与他的家庭都感到十分欣慰. 另外，在 1947 年他的女儿华苏出生了；在这之前，他还有两个儿子华陵与华光，后者生于 1945 年，稍晚，还有一个华密. 1948 年春，华罗庚接受了作为位于乌尔班那–香槟的伊利诺伊大学正教授的聘请. 在那里他指导了阿尤布 (R. Ayoub) 的博士论文

(后来, 阿尤布成为宾州州立大学的教授); 继续与赖纳的合作; 并影响了几个年轻研究人员的思路, 其中包括舍内菲尔德 (L. Schoenefeld) 与米切尔 (J. Mitchell). 华罗庚待在伊利诺伊的时间是很短暂的, 中国正发生着巨大的变化, 华罗庚热切地注视着事态的发展而且愿意投身于这一新时代中. 尽管他与妻子及三个年幼的孩子在乌尔班那安顿得非常舒适, 他回归的冲动却异常激烈. 1950 年 3 月 16 日, 他回到了北京他的母校清华大学, 准备对这美好的新世界作出他自己的贡献. 那时, 他正处于他的数学才智之巅. 正如在许多年后, 他给我的信中所说, 回顾起来, 40 年代对他而言, 是一生中的黄金岁月. 尽管他需要面对种种困难, 他从未对他的回国决定后悔过.

回到中国后, 华罗庚即投身到教学改革当中, 组织各种不同层次的数学活动, 指导研究生①, 到中学做报告, 以及到新兴工业部门中给工人们讲课. 1952 年 7 月中国科学院数学研究所开办了, 华罗庚被任命为首任所长. 次年, 他作为中国科学院访苏代表团的 26 名成员之一访问了苏联. 代表团企图建立与俄国科学的联系, 这时, 华罗庚曾疑惑共产党是否信任他, 但在莫斯科时, 当他得知中国政府已同意苏联政府将斯大林奖金授予华罗庚的建议, 这对他确是十分惊喜的事. 但在斯大林去世后, 奖励被中止, 华罗庚也就失去了得奖的机会. 对于以后的发展, 华罗庚告诉我, 他倍感满意!

除了许多数学与行政职务外, 华罗庚的研究工作仍很活跃, 并继续写作, 其中不仅在他进行过的领域, 也包括一些对他来说是新的, 或以前稍有过接触的领域. 1956 年, 他的巨型教科书《数论导引》出版了 (根据政府命令, 1975 年中文版的序言被删去, 这是由于华罗庚在文化大革命中大部分时间靠边站了); 以后施普林格出版社出版了这本书的英文版, 而且该书仍在继续再版之中. 1958 年出版了《多复变函数论中的典型域的调和分析》, 同年这本书被译成俄文出版, 接着 1963 年美国数学会出版了它的英文译本. 这本重要专著中的绝大部分结果都是属于华罗庚本人的, 其中与西格尔的工作有某些重复. 这本书的结果对表示理论、齐性空间理论与自守形式理论都有应用. 这本专著也包含他与陆启铿合作的关于泊松 (S. D. Poisson) 与伯格曼 (S. Bergman) 核的工作. 华罗庚的这项工作以后对于施泰因 (E. Stein) 关于全纯函数的边界性质的研究是有用的. 1959 年华罗庚给予了将霍奇 (W. W. D. Hodge) 理论推广至开埃尔米特 (C. Hermite) 流形以重要评价; 1962 年科恩 (J. J. Kohn) 成功地完成了这项工作. 早先提到的 1959 年出版的关于指数和的专著亦被译成俄文出版了. 华罗庚是一位深入浅出与多产的作家, 为了使学生易于进入近代数学, 他用中文为学校及大学生写了很多书与文章. 为了自述情怀及朋友们的愉悦, 他终身都在写诗.

---

① 在他的学生中, 数论方面有陈景润、潘承洞与王元; 代数方面有万哲先; 分析方面有龚昇与陆启铿.

1958 年, 华罗庚在所谓 "大跃进" 乌托邦的美梦中被猛然唤醒. 毛泽东鼓励向知识分子的猛烈攻击横扫了全国, 在 "卑贱者最聪明, 高贵者最愚蠢" 这样的口号激励下, 由顺从的政府官员满怀热情地予以实施. 除了他的高位和来自高层的保护外, 华罗庚遭到了折磨、公开的谩骂与不断的监视, 然而就在这样骚乱的时期, 华罗庚与王元一起发展了线性规划、运筹学与高维数值积分等广泛的课题. 关于最后这个方面, 由于蒙特卡罗 (Monte Carlo) 方法的研究与一致分布的作用促使他们去创造了一个基于代数数论的不同的决定性方法, 他们的理论含于著作《数论在近似分析中的应用》之中. 这本书出版得相当晚, 直到 1978 年才面世. 1981 年, 施普林格出版社出版了英文译本. 新建立的应用数学兴趣使华罗庚在 60 年代带着一个小分队跑遍全国, 向各种工人传授如何将他们的知识技能用于工厂与日常生活的问题, 不管在工厂的问题解答会上或现场教学中, 他用数学精神感染了他的听众到了这样的程度, 从而使他成了一个民族英雄, 甚至毛泽东主动给他写了一封赞扬信, 这为他在动乱时期提供了宝贵的保护. 华罗庚仪表堂堂, 和蔼可亲, 有一种将事理简化的奇异手段, 从而随着他旅行的影响, 他的盛名广传而且数学的声誉也遍及全国①, 当较晚他出国旅行时, 各种政治信仰的中国人群都争相拜会他并向他致敬. 1984 年, 当他在杭州举办一个多复变函数论会议时, 西方同行对中国新闻媒体宣传的规模甚感惊奇.

但所有这些都是未来的事了. 1966 年, 毛泽东发动了另一全国性灾难的运动, 即延续了十年之久的所谓 "文化大革命", 早在 1965 年 6 月 26 日, 毛泽东在一次讲话中, 即向知识分子传递了一个不祥的信息: "书读得愈多愈愚蠢". 华罗庚许多年实际上处于软禁中, 他将他的生存归功于周恩来亲自出面对他的保护. 即使这样, 他仍然遭到不断侵扰的质询. 他的一些手稿 (数学经济) 被查抄了, 而且永远丢失了. 他的同事与以前的学生被发动起来发表攻击他的言论 (在 1978 年, 中国驻英大使向我叙述了这样一个场面: 可能是下一代中国最为知晓的数学家陈景润被命令站在一个公共场所几小时, 一群造反派围着他, 要他揭露华罗庚. 当时也在场的陈景润插话说, 实际上他很喜欢这一机会, 因为没有学生会用无聊的问题来打扰他, 因此他有时间可以毫无干扰地想数学问题了!). 这的确不奇怪, 1965 年华罗庚就过早地停止发表著作了. 当然, 他仍然在工作, 他还有几篇关于近似分析的合作文章 (与王元) 及最优化文章 (登于《科学通报》, 发表于 70 年代). 这些工作或许是基于他早先做的工作而写成的, 也有些他多年在广泛的教学与咨询经验中提取积累而写成的综合论文与教科书. 他在 1981 年的一篇文章中, 悲伤地回顾道 "谁知步入第十六个年头的时候, 我被 …… 弄得走投无路, 几乎精疲力尽".

随着 1976 年 "文化大革命" 的结束, 华罗庚进入了他生命的最后阶段, 在国内

① 关于处理过的问题精选请见 *Popularizing Mathematical Methods in the People's Republic of China.* by L. K. Hua and Y. Wang. Boston: Birkhäuser, 1989.

他恢复了荣誉. 他被任命为中国科学院副院长、全国人民代表大会代表及政府的科学顾问, 除此之外, 中央电视台 (CCTV) 拍了一个短的电视系列剧来讲述华罗庚一生的故事. 这一电视剧至少被播放了两次. 1980 年, 他扮演着他国家的文化大使, 重建与西方学术界的联系, 在往后的五年中, 他遍访了欧洲、美国与日本, 1979 年, 他是英国科学研究委员会设于伯明翰大学的一位研究员, 在 1983—1984 年, 他作为一位杰出学者 (Sherman fairchild distinguished scholar) 在加州理工学院停留, 绝大多数时间里, 他都很疲倦并且健康欠佳, 但他并未丧失对生命的情趣与无限的好奇心. 1984 年春他在乌尔班那对一大堆听众报告他的数学经济工作, 人们感到他在加紧努力以补偿他丢失的岁月, 1985 年 5 月 21 日在他给我的最后信件中, 他告诉我, 现在的绝大部分时间都在不幸地从事 "非数学活动, 而这些活动对他的国家与人民都是必需的". 1985 年 6 月 12 日在东京的一次演讲结束时, 他逝世于心脏病发作.

华罗庚得到南锡大学 (1980 年)、香港中文大学 (1983 年) 与伊利诺伊大学 (1984 年) 的荣誉博士. 他被选为美国国家科学院外籍院士 (1982 年)、德国自然科学院 (Deutsche Akademie der Naturforscher Leopoldia)(1983 年)、第三世界科学院 (1983 年) 与巴伐利亚科学院 (Bavarian Academy of Sciences)(1985 年) 院士.

王元教授为华罗庚写过一个很好的传记①, 我对能用到这本书的一些材料表示感谢, 我也曾为《算术学报》(*Acta Arithmetica*) 写过一篇悼念他的文章 (LI(1988): 99—117).

① Y. Wang, Hua Loo-keng. Translated by Peter Shiu. Singapore: Springer, 1999.

# 著作精选

**1936**

With S. S. Shu. On Fourier transforms in $L^p$ in the complex domains. *J. Math.* Phys, 15: 249–263.

**1938**

On Waring's problem. *Q. J. Math.*, 9: 199–202.

On the representation of numbers as the sums of the powers of primes. *Math. Z.*, 44: 335–346.

**1940**

On an exponential sum. *J. Chin. Math. Soc.*, 2: 301–312.

With H. F. Tuan. Some "Anzahl" theorems for groups of prime-power orders. *J. Chin. Math. Soc.*, 2: 313–319.

**1942**

On the least primitive root of a prime. *Bull. Am. Math. Soc.*, 48: 726–730.

The Lattice-points in a circle. *Q. J. Math.*, 13: 18–29.

**1944**

On the theory of automorphic functions of a matrix variable. I. Geometrical basis. II. The classification of hypercircles under the symplectric group. *Am. J. Math.*, 66: 470–488, 531–563.

**1945**

Geometries of matrices. I. Generalizations of von Staudt's theorem. II. Arithmetical construction. *Trans. Am. Math. Soc.*, 57: 441–481, 482–490.

**1946**

Orthogonal classification of Hermitian matrices. *Trans. Am. Math. Soc.*, 59: 508–523.

**1947**

Geometries of matrices. III. Fundamental Theorems in the geometries of symmetric

matrices. *Trans. Am. Math. Soc.*, 61: 229–255.
With S. H. min. On a double exponential sum. *Sci. Rep. Tsing Hua Univ.*, A4: 484–518.

**1948**

On the automorphisms of the symplectic group over any field. *Ann. Math.*, 49: 739–759.

**1949**

On the automorphisms of a sfield. *Proc. Nat. Acad. Sci. U. S. A.*, 35: 386–389.
Some properties of a sfield. *Proc. Nat. Acad. Sci. U. S. A.*, 35: 533–537.
An improvement of Vinogradov's mean-value theorem and several applications. *Q. J. Math.*, 20: 48–61.

**1951**

Supplement to the paper of Dieudonné on the automorphisms of classical groups. *Mem. Am. Math. Soc.*, 2: 96–122.
With I. Reiner. Automorphisms of the unimodular group. *Trans. Am. Math. Soc.*, 71: 331–348.

**1957**

On exponential sums. *Sci Rec.* (*N. S.*), 1(1): 1–4.
On the major arcs of Waring problem. *Sci. Res.* (*N. S.*), 1(3): 17–18.
On the Riemannian curvature in the space of several complex variables. *Schr. Forschungsinst. Math.*, 1: 245–263.

**1959**

*Abschätzungen von Exponentialsummen und ihre Anwendung in der Zahlentheorie.* Leipzig: Teubner. (Chinese translation: Peking: Academic Press, 1963; Rus-sian translation: Moskva: Mir, 1964.)

**1963**

*Harmonic Analysis of Functions of Several Complex Variables in the Classical Domains* (English translation). Providence, R. I.: American Mathematical Society(In Chinese: Peking: Academic Press, 1958, rev. ed., 1965; Russian translation: Moskva: Izd. Inostran. Lit., 1959).

**1965**

Additive theory of prime numbers (English translation). Providence. R. I.: American Mathematical Society(In Russian: *Trudy Inst. Math. Steklov*, 22(1947): 1–179; Chinese translation [revised]: Peking: Academic Press, 1957; Hungarian translation: Budapest: Académiai Kiadó, 1959; German translation: Leipzing: Teuber, 1959).

**1981**

With Y. Wang . *Application of Number Theory to Numerical Analysis* (English translation). New York: Springer(In Chinese: Peking: Academic Press, 1978.)

# 关于多变量堆垒数论的一个问题[1]

华罗庚[2](中国，北平)

本文将回答如下的问题:

设 $P(x,y)$ 和 $P'(x,y)$ 为两个整值多项式, $\varepsilon_\nu=\pm1$. 是否存在一个正整数 $s$, 使得对于所有的整数 $n$ 和 $n'$, 丢番图方程组

$$\begin{cases}\sum_{\nu=1}^{s}\varepsilon_\nu P(x_\nu,y_\nu)=n,\\ \sum_{\nu=1}^{s}\varepsilon_\nu P'(x_\nu,y_\nu)=n'\end{cases}\tag{1}$$

总有解?

如果 $P$ 和 $P'$ 满足某个限制条件, 则问题的答案是肯定的. 这里还将给出 $s$ 的上界, 它等于 $2^k k-1$, 其中 $k$ 为 $P$ 与 $P'$ 的次数的最大者.

我们假设: $P(x,y)$ 和 $P'(x,y)$ 为两个整值多项式, 次数分别为 $k$ 和 $k'$. 对于任一个素数 $p$, 不存在整数 $q,q'((q,q')=1)$ 和 $l$, 使得

$$qP(x,y)+q'P'(x,y)\equiv l(\text{mod}p)\tag{2}$$

恒等地成立. 不失一般性, 我们可设 $k\geqslant k'$. 在本问题里, 上述限制条件不能够去掉, 否则, $n$ 和 $n'$ 将无法取到任意的整数.

**引理 1** 每一个整值多项式 $P(x,y)$ 都可以表作

$$P(x,y)=\sum a_{\mu,\nu}P_\mu(x)P_\nu(y),$$

其中 $a_{\mu,\nu}$ 为整数, 而

$$P_\mu(z)=\frac{z(z-1)\cdots(z-\mu+1)}{\mu!}\quad(\mu>0),\quad P_0(z)=1.$$

**引理 2** 令

$$P(x,y)=\sum a_{\mu,\nu}P_\mu(x)P_\nu(y)$$

① 1936 年 4 月 20 日收到. 发表于 *Mathematische Zeitschrift*, 1936, 41(5): 708–712.
② 时任中华教育与文化促进基金会研究员.

和

$$P'(x,y)=\sum a'_{\mu,\nu}P_\mu(x)P_\nu(y).$$

对于给定的素数 $p$, 存在整数 $q,q'$ 和 $l$, 使得

$$qP(x,y)+q'P'(x,y)\equiv l(\mathrm{mod}p)$$

恒等地成立的充分必要条件是

$$\begin{aligned}&qa_{\mu,\nu}+q'a'_{\mu,\nu}\equiv 0(\mathrm{mod}p),\quad (\mu,\nu)\neq(0,0),\\&qa_{0,0}+q'a'_{0,0}\equiv l(\mathrm{mod}p).\end{aligned}$$

用作者以前的文章①里的方法, 可以容易地得到这两个引理.

用 $H(P,P',m,m')$ 记最小的正整数 $s$, 使得对于所有的整数 $n$ 和 $n'$, 同余方程组

$$\begin{cases}\displaystyle\sum_{\nu=1}^{s}\varepsilon_\nu P(x_\nu,y_\nu)\equiv n(\mathrm{mod}m),\\ \displaystyle\sum_{\nu=1}^{s}\varepsilon_\nu P'(x_\nu,y_\nu)\equiv n'(\mathrm{mod}m')\end{cases}$$

总有解. 而 $H(P,P',0,0)$ 即为使方程组 (1) 有解的最小正整数 $s$.

用 $\Delta_t^x(P(x,y))$ 和 $\Delta_t^y(P(x,y))$ 分别表示 $P(x,y)$ 关于 $x$ 与 $y$ 的 $t$ 阶差分. $\Delta_t^x(P(x,y))$ 可以写成 $2^t$ 个形如 $\pm P(x,y)$ 的项之和.

**引理 3** 设 $\alpha,\beta,\gamma$ 和 $\delta$ 为整数, 满足

$$\begin{vmatrix}\alpha & \beta\\ \gamma & \delta\end{vmatrix}=\pm1,$$

则

$$H(P,P',0,0)=H(\alpha P+\beta P',\gamma P+\delta P',0,0).$$

本引理立即可得.

**引理 4** 设 $a_{u,v}P_u(x)P_v(y)$ 为 $P(x,y)$ 的 $k$ 次项中的一项. 如果 $a'_{u,v}=0$, 而 $P'\not\equiv 0(\mathrm{mod}m)$, 则有

$$H(P,P',m,m')\leqslant 2^{k-1}+H(P,P',(m,a_{u,v}),m'),$$

这里 $m$ 或 $m'$ 可以为 0.

---

① *J. London Math. Soc.*, 1935, 11: 4–5. *Science Report of Tsing Hua University, Ser.A*, 1935, 3: 247–260.

**证明** 此时,

$$\Delta_{u-1}^{x}\Delta_{v}^{y}P(x,y)=a_{u,v}x+a_{u-1,v}+a_{u-1,v+1}y,$$
$$\Delta_{u-1}^{x}\Delta_{v}^{y}P'(x,y)=a'_{u-1,v}+a'_{u-1.v+1}y.$$

令 $s$ 为一个 $\geqslant H(P,P',(m,a_{u,v}),m')$ 的整数, 则对于所有的整数 $n$ 和 $n'$, 方程组

$$\begin{cases}\sum_{\nu=1}^{s}\varepsilon_{\nu}P(x_{\nu},y_{\nu})\equiv n(\bmod(m,a_{u,v})),\\ \sum_{\nu=1}^{s}\varepsilon_{\nu}P'(x_{\nu},y_{\nu})\equiv n'(\bmod m')\end{cases}$$

总有解. 因此, 有

$$\begin{cases}\sum_{\nu=1}^{s}\varepsilon_{\nu}P(x_{\nu},y_{\nu})+\Delta_{u-1}^{x}\Delta_{v}^{y}P(x,y)\equiv N(\bmod m),\\ \sum_{\nu=1}^{s}\varepsilon_{\nu}P'(x_{\nu},y_{\nu})+\Delta_{u-1}^{x}\Delta_{v}^{y}P'(x,y)\equiv N'(\bmod m')\end{cases}\tag{3}$$

(对于所有的整数 $N$ 和 $N'$ 可解). 事实上, (3) 式可以写成

$$\begin{cases}\sum_{\nu=1}^{s}\varepsilon_{\nu}P(x_{\nu},y_{\nu})+a_{u,v}x+a_{u-1,v}+a_{u-1,v+1}y\equiv N(\bmod m),\\ \sum_{\nu=1}^{s}\varepsilon_{\nu}P'(x_{\nu},y_{\nu})+a'_{u-1,v}+a'_{u-1,v+1}y\equiv N'(\bmod m').\end{cases}$$

由 (3) 式和引理 3 前面的解释, 可得本引理.

**引理 5**

$$H(P,P',0,0)\geqslant H(P,P',m,m').$$

本引理是显然的.

**引理 6** 令

$$R(x,y)=ax+by+c,$$
$$R'(x,y)=a'x+b'y+c'.$$

如果对于任一个素数 $p$, 不存在整数 $q,q'((q,q')=1)$ 和 $l(>1)$, 使得

$$qR(x,y)+q'R'(x,y)\equiv l(\bmod p),$$

则

$$\begin{vmatrix} a & a' \\ b & b' \end{vmatrix} = \pm 1.$$

因此

$$H(R, R', 0, 0) = H(x, y, 0, 0) = 1.$$

**证明** 取 $\mu$ 和 $\mu'$ 为两个整数, 使得

$$a\mu + a'\mu' = 0, \quad (\mu, \mu') = 1.$$

则有

$$b\mu + b'\mu' = \pm 1.$$

不然的话, 令 $p$ 为 $b\mu + b'\mu'$ 的一个素因子, 于是,

$$\mu R(x, y) + \mu' R'(x, y) \equiv \mu c + \mu' c' (\bmod p)$$

恒等地成立, 但这与我们的假设相矛盾. 因此, $(b, b') = 1$. 相似地, $(a, a') = 1$. 所以, 我们有

$$\begin{vmatrix} a & a' \\ b & b' \end{vmatrix} = \pm 1.$$

**定理 1**

$$H(P, P', 0, 0) \leqslant 2^k k - 1.$$

**证明** 令 $a_{u,v} P_u(x) P_v(y)$ 为 $P(x, y)$ 的一项, 这里 $u + v = k, a_{u,v} \neq 0$, 而 $u$ 为满足条件 $u + v = k$ 的 $u$ 的最大者.

1. $a'_{u,v} = 0$.

由引理 4 和 5 可得

$$\begin{aligned} H(P, P', 0, 0) &\leqslant 2^{u+v-1} + H(P, P', a_{u,v}, 0) \\ &\leqslant 2^{k-1} + H(Q, Q', 0, 0), \end{aligned}$$

这里 $Q$ 和 $Q'$ 为两个与 $P$ 和 $P'$ 有相同性质的多项式, 且

$$P \equiv Q, \quad P' \equiv Q' (\bmod a_{u,v}),$$

而 $P_u(x) P_v(y)$ 在 $Q$ 和 $Q'$ 中的系数均为 0.

2. $a'_{u,v} \neq 0$.

取 $r, r'$ 为两个整数, 具有性质

$$(r, r') = 1$$

和

$$ra_{u,v}+r'a'_{u,v}=0.$$

又取整数 $s, s'$ 使得

$$\begin{vmatrix} r & r' \\ s & s' \end{vmatrix} = \pm 1.$$

由引理 3, 我们有

$$H(P,P',0,0)=H(sP+s'P',rP+r'P',0,0),$$

而 $P_u(x)P_v(y)$ 在 $rP+r'P'$ 中的系数为 0. 由情形 1 中的讨论知, 有两个多项式 $Q$ 和 $Q'$(它们与 $P$ 和 $P'$ 有相同的性质, 且其中的 $P_u(x)P_v(y)$ 的系数均为 0) 使得

$$\begin{aligned} H(P,P',0,0) &\leqslant 2^{u+v-1}+H(Q,Q',0,0) \\ &\leqslant 2^{k-1}+H(Q,Q',0,0). \end{aligned}$$

这在两种情形里都对.

不断重复这个过程, 我们最终得到

$$H(P,P',0,0)\leqslant \sum_{\nu=2}^{k}(\nu+1)2^{\nu-1}+H(R,R',0,0),$$

其中 $R(x,y)$ 和 $R'(x,y)$ 为引理 6 中论及的两个线性多项式. 因此, 我们有

$$H(P,P',0,0)\leqslant \sum_{\nu=1}^{k}(\nu+1)2^{\nu-1}-1=k2^k-1.$$

这个结果可以推广到 $t$ 个变量:

**定理 2** 设 $P_1,\cdots,P_t$ 为变量是 $x_1,\cdots,x_t$ 的 $t$ 个整值多项式, 其次数最高者为 $k$. 假设对于任一个素数 $p$, 不存在整数 $q_1,\cdots,q_t$ 和 $l(>1)$, 使得

$$q_1P_1+\cdots+q_tP_t\equiv l(\mathrm{mod}p),\quad (q_1\cdots,q_t)=1.$$

则有

$$H(P_1,\cdots,P_t,0,\cdots,0)=O(2^kk^{t-1}).$$

(贾朝华 译)

# 多变量堆垒数论中的一个问题①

华罗庚②

在试图解决由 Mordell 教授的工作③引申出来的一个问题时，我得到了下面的结果.

设④

$$F_1(x,y), F_2(x,y), \cdots, F_{k+1}(x,y)$$

为 $k+1$ 个 $k$ 次整值多项式. 众所周知, $F_i(x,y)$ 可以表作

$$F_i(x,y) = \sum_{\substack{\mu+\nu\leqslant k\\ \mu\geqslant 0\\ \nu\geqslant 0}} a_{\mu,\nu}^{(i)} P_\mu(x) P_\nu(y),$$

其中 $a_{\mu,\nu}^{(i)}$ 为整数, 而

$$P_\mu(x) = \frac{x(x-1)\cdots(x-\mu+1)}{\mu!} \quad (\mu > 0), \quad P_0(x) = 1.$$

令

$$\begin{vmatrix} a_{0,k}^{(1)} & \cdots & a_{k,0}^{(1)} \\ \vdots & & \vdots \\ a_{0,k}^{(k+1)} & \cdots & a_{k,0}^{(k+1)} \end{vmatrix} = \Delta,$$

于是, 我们有

**定理 1** 如果 $\Delta \neq 0$, 则存在整数 $m_1, \cdots, m_{k+1}$ 和 $N$, 使得对于任一组整数 $n_i \equiv m_i (\bmod |\Delta|)$, 我们可以找到整数 $x_i, y_i$ 和适当的 $\varepsilon_i = \pm 1$, 满足

$$\sum_{i=1}^{N} \varepsilon_i F_j(x_i, y_i) = n_j \quad (j = 1, \cdots, k+1).$$

我们可取 $N = \left[\frac{k}{2}+1\right] 2^{k-1}$.

---

① 1936 年 11 月 1 日收到, 1936 年 11 月 12 日审阅. 发表于 *Journal of the London Mathematical Society*, 1937, 12: 257–261.

② 时任中华教育与文化促进基金会研究员.

③ *J.London Math.Soc.*, 1936, 11: 204–208.

④ 当多项式为两个的时候, 作者有更细致的结果, 发表在*Math.Zeitschrift*, 1936, 41: 708–712.

**证明** 存在整数 $b_{i,j}(1 \leqslant i,j \leqslant k+1)$, 使得多项式

$$Q_i(x,y) = \sum_{j=1}^{k+1} b_{i,j} F_j(x,y) \quad (\text{行列式}|b_{i,j}| = \pm 1)$$

有下面的特殊形式:

$$Q_i(x,y) = \sum_{\substack{\mu+\nu \leqslant k \\ \mu \geqslant 0 \\ \nu \geqslant 0}} A_{\mu,\nu}^{(i)} P_\mu(x) P_\nu(y),$$

$$A_{j,k-j}^{(i)} = 0, \quad \text{当 } j+1 < i \text{ 时},$$

$$A_{0,k}^{(1)} \cdots A_{k,0}^{(k+1)} = \Delta.$$

容易验证, 如果定理对于 $Q_i(x,y)$ 成立, 则它对 $F_i(x,y)$ 也成立.

对于任一个整值多项式 $R(x,y)$, 用 $\Delta_t^x(R(x,y))$ 和 $\Delta_t^y(R(x,y))$ 分别表示 $R(x,y)$ 关于 $x$ 与 $y$ 的 $t$ 阶差分. $\Delta_t^x(R(x,y))$ 可以写成 $2^t$ 个形如 $\pm R(x,y)$ 的项之和.

(1) $k$ 为奇数.

考虑 $k+1$ 个表达式

$$\Delta_{k-1}^y Q_i(x_1,y_1) + \Delta_{k-3}^y \Delta_2^x Q_i(x_2,y_2) + \cdots + \Delta_{k-1}^x Q_i(x_{\frac{1}{2}(k+1)}, y_{\frac{1}{2}(k+1)}),$$

这里 $i = 1, 2, \cdots, k+1$. 它们可以简化为一组线性形式

$$A_{0,k}^{(1)} y_1 + A_{1,k-1}^{(1)} x_1 + A_{2,k-2}^{(1)} y_2 + A_{3,k-3}^{(1)} x_2 + \cdots + m_1,$$

$$A_{1,k-1}^{(2)} x_1 + A_{2,k-2}^{(2)} y_2 + A_{3,k-3}^{(2)} x_2 + \cdots + m_2,$$

$$\cdots\cdots$$

其中 $m_1, m_2, \cdots$ 为常数. 因为

$$A_{0,k}^{(1)} A_{1,k-1}^{(2)} \cdots A_{k,0}^{(k+1)} = \Delta,$$

所以, 对于任一组整数 $n_i \equiv m_i (\bmod |\Delta|)$, 线性方程组

$$\Delta_{k-1}^y Q_i(x_1,y_1) + \cdots + \Delta_{k-1}^x Q_i(x_{\frac{1}{2}(k+1)}, y_{\frac{1}{2}(k+1)}) = n_i \quad (i = 1, \cdots, k+1)$$

有整数解. 因此, 当 $N = (k+1)2^{k-2}$ 时, 我们可以解出定理中的方程组.

(2) $k$ 为偶数.

通过考虑

$$\Delta_{k-1}^y Q_i(x_1,y_1) + \Delta_{k-3}^y \Delta_2^x Q_i(x_2,y_2) + \cdots$$

$$+\Delta_1^y\Delta_{k-2}^x Q_i(x_{\frac{1}{2}k},y_{\frac{1}{2}k})+\Delta_{k-1}^x Q_i(x_{\frac{1}{2}k+1},0),$$

我们可以用与情形 (1) 中相同的方式得出结果, 此时, $Q(x,y)$ 的个数为 $(k+2)2^{k-2}$.

**推论** 如果 $\Delta=\pm1$, 则存在一个整数 $N$, 使得方程组

$$\sum_{i=1}^{N}\varepsilon_i F_j(x_i,y_i)=n_j\quad(\varepsilon_i=\pm1,j=1,\cdots,k+1)$$

对于任一组整数 $n_j$ 均可解.

例如, 一组多项式

$$G_i(x,y)=P_i(x)P_{k-i}(y)\quad(i=1,\cdots,k+1)$$

满足以上的条件.

如果要找一个 $N$, 使得

$$n_1X^k+n_2X^{k-1}Y+\cdots+n_{k+1}Y^k=\sum_{i=1}^{N}\varepsilon_i(x_iX+y_iY)^k$$

有解, 就相当于在上面讨论的问题里取

$$F_1(x,y)=x^k,F_2(x,y)=kx^{k-1}y,\cdots,F_{k+1}(x,y)=y^k.$$

注意此时,

$$\begin{aligned}&\Delta_{k-i}^x\Delta_{i-1}^y F_j(x,y)\\&=\frac{k!}{(j-1)!(k-j+1)!}\Delta_{k-i}^x\Delta_{i-1}^y(x^{k-j+1}y^{j-1})\\&=\begin{cases}k!x, & \text{当 } j=i \text{ 时},\\ k!y, & \text{当 } j=i+1 \text{ 时},\\ 0, & \text{其他}.\end{cases}\end{aligned}$$

因此, 当 $k$ 为奇时,

$$\sum_{i=1}^{\frac{1}{2}(k+1)}\Delta_{k-2i+1}^x\Delta_{2i-2}^y F_j(x_i,y_i)=\begin{cases}k!x_{\frac{1}{2}(j+1)}, & \text{当 } j \text{ 为奇时},\\ k!y_{\frac{1}{2}j}, & \text{当 } j \text{ 为偶时};\end{cases}$$

而当 $k$ 为偶时,

$$\sum_{i=1}^{\frac{1}{2}k}\Delta_{k-2i+1}^x\Delta_{2i-2}^y F_j(x_i,y_i)+\Delta_{k-1}^y F_j(x_{\frac{1}{2}k+1},0)=\begin{cases}k!x_{\frac{1}{2}(j+1)}, & \text{当 } j \text{ 为奇时},\\ k!y_{\frac{1}{2}j}, & \text{当 } j \text{ 为偶时}.\end{cases}$$

用前面的方法, 我们有

**定理 2**　任一个二元 $k$次型, 如果它的系数为 $k!$ 的倍数, 则它可以表作至多 $\left[\frac{1}{2}k+1\right]2^{k-2}$个整系数线性型的 $k$ 次幂的和或差.

定理 2 表明, 在考虑用线性型的 $k$ 次幂的和或差表示一个型时, 只需将型的系数限制在 0 和 $k!$ 之间即可. 因为这里给出的上界不是最小可能的, 所以, 可以通过检查系数小于 $k!$ 的型, 使 Mordell 教授叙述的问题得到部分的解决.

看来要将这种方法推广到两个变量以上并不容易. 下面的方法比较简单 (但所得到的上界较大), 可以推广到两个变量以上.

因为

$$\begin{aligned}&\Delta_{k-1}^{y}F_i(0,y_1)+\Delta_{k-2}^{y}\Delta_1^{x}F_i(0,y_2)+\cdots\\&+\Delta_1^{y}\Delta_{k-2}^{x}F_i(0,y_{k-1})+\Delta_{k-1}^{x}F_i(x,y_k)\\=\ &a_{0,k}^{(i)}y_1+a_{1,k-1}^{(i)}y_2+\cdots+a_{k-1,1}^{(i)}y_k+a_{k,0}^{(i)}x+m_i,\end{aligned}$$

这里 $m_i$ 为整数, 所以, 对于 $N=k2^{k-1}, n_i\equiv m_i(\mathrm{mod}|\Delta|)$, 丢番图方程组

$$\sum_{i=1}^{N}\varepsilon_iF_j(x_i,y_i)=n_j\quad(j=1,\cdots,k+1)$$

有解.

在 $n$ 个变量问题里, 所对应的上界是

$$\frac{1}{n!}k(k+1)\cdots(k+n)2^{k-1}.$$

运用这种方法, 我们可得下面的结果:

**定理 3**　令 $\beta$ 是一个有限环, 它没有幂零元, 环的基为 $\omega_1,\cdots,\omega_n$. 则存在整数 $m,N$ 和环中的一个元 $\omega$, 使得环中任一个同余于 $\omega(\mathrm{mod}m)$ 的元都可表作 $N$ 个 $X^k$ 的和或差, 而这些 $X$ 均为环中的元.

设

$$X=x_1\omega_1+\cdots+x_n\omega_n$$

和

$$X^k=y_1\omega_1+\cdots+y_n\omega_n,$$

这里 $y_i$ 是变量为 $x_1,\cdots,x_n$ 的 $k$ 次齐次多项式. 令 $R$ 为 $y_i$ 的结式, 则

$$y_1=0,\cdots,y_n=0$$

有非平凡解的充分必要条件是 $R=0$. 因为环没有幂零元, 所以, 我们有 $R\neq 0$. 因此, 不存在不全为零的整数 $l_1,\cdots,l_n$, 使得

$$l_1y_1+\cdots+l_ny_n=0$$

恒等地成立. 用我们先前的讨论, 可得定理.

在此, 我要感谢 Mordell 教授的鼓励.

(贾朝华　译)

# 关于一个推广的华林问题①

华罗庚②

## 1. 引　　言

在本文的第一部分里, 我们希望找到华林问题中的 Hardy-Littlewood 渐近公式对于多项式的推广, 即要求丢番图方程

$$N = P_1(h_1) + \cdots + P_s(h_s) \quad (h_\nu \geqslant 0) \tag{1}$$

的解数公式, 这里 $P_\nu$ 均为 $k$ 次整值多项式, 首项系数为正. 我们所用的方法本质上属于 Vinogradov[3]. 在优弧的处理上, 采用了 Heilbronn[1] 的方法.

令 $G\{P(h)\}$ 为最小的正整数 $s$, 使得当 $N$ 充分大时, 方程 (1) 对于 $P_1(h) = P_2(h) = \cdots = P_s(h) = P(h)$ 有解③. 而 $P(h)$ 必须满足条件: 如果 $q(>1)$ 是一个整数, 则不存在整数 $d$, 使得

$$P(h) \equiv d (\bmod q)$$

恒等地成立.

关于 $G\{P(h)\}$ 的主要结果如下.

**定理 A**　如果 $P(h)$ 为奇的 $k$ 次整值多项式, 而 $k > 20$, 则有

$$G\{P(h)\} \leqslant \frac{1}{3}(2^{k+1} - 1).$$

进一步地, 如果 $P(h)$ 的首项系数为 $a/k!, (a, k!) = 1$, 则对于任给的 $\varepsilon > 0$, 有

$$G\{P(h)\} = O(2^{\varepsilon k}).$$

这相当于定理 5 和 6 合在一起.

**定理 B**　如果 $P(h)$ 为 $k$ 次整值多项式, 而 $k > 20$, 则有

$$G\{P(h)\} \leqslant 3^{\frac{k}{2}} 2^{\frac{1}{2}(k-1)+7} k$$

---

① 1936 年 6 月 29 日收到, 1936 年 11 月 12 日审阅, 1937 年 3 月 23 日收到修改稿. 发表于 *Proceedings of the London Mathematical Society*, 1937, 43(2): 161–182.

② 时任中华教育与文化促进基金会研究员.

③ 关于不同的 $P_\nu$ 的研究, 将在以后给出.

和

$$G\{P(h)\} = O(k^3 2^{k-1}).$$

进一步地, 如果 $P(h)$ 的首项系数为 $a/k!, (a, k!) = 1$, 则对于任给的 $\varepsilon > 0$, 有

$$G\{P(h)\} = O(3^{k(\frac{1}{2}+\varepsilon)}).$$

这相当于定理 7,8 和 9 合在一起.

Kamke[1] 最先证明了 $G\{P(h)\}$ 上界的存在性, 但还没人给出它的确定值.

本文所遇到的主要困难是算术的而非分析的. 在某些情况中, 我引用了稍加推广后的 Vinogradov 或其他作者的分析定理, 其中一些必要的改造是不困难的.

借此机会, 我要感谢 Heilbronn 博士的鼓励和指点.

## 2. 记　　号

令 $r(N) = r_{P_1,\cdots,P_s}(N)$ 为丢番图方程

$$N = P_1(h_1) + P_2(h_2) + \cdots + P_s(h_s) \quad (h_\nu \geqslant 0, \nu = 1, 2, \cdots, s)$$

的解数, 其中 $P_\nu(h)(\nu = 1, 2, \cdots, s)$ 为 $k$ 次整值多项式, 所有系数均为正, 而常数项为零①.

设 $N_\nu$ 为 $P_\nu(h) = N(>0)$ 的最大正根, 它存在且随 $N$ 趋向无穷.

$k$ 是整数. $b = k/(k+1)$.

$q_\nu^*$ 表示 $q$ 关于 $P_\nu(h)$ 的连接数②.

我们记

$$\mathrm{e}^{2\pi \mathrm{i} x} = e(x), \quad \rho = e\left(\frac{l}{q}\right), \quad (l, q) = 1,$$

$$S_{\rho,\nu} = \sum_{h=0}^{q_\nu^*} \rho^{P_\nu(h)} \quad (\nu = 1, 2, \cdots, s),$$

$$A(q) = A_s(q, j) = \sum_{\rho} \left(\prod_{\nu=1}^{s} \frac{S_{\rho,\nu}}{q_\nu^*}\right) \rho^{-j},$$

这里 $\rho$ 过所有 $q$ 次本原单位根. 以下如果没有特别的说明, $\prod$ 和 $\sum$ 总表示 $\prod_{\nu=1}^{s}$

① 这里唯一本质性的限制是每个多项式的首项系数为正. 由此, 我们总可以取整数 $l$ 充分大, 使得 $Q_\nu(h) = P_\nu(h+l)$ 的所有系数均为正.

② 见 Hua[3, 4].

和 $\sum_{\nu=1}^{s}$,

$$\mathcal{S}(n)=\sum_{q=1}^{\infty}A_s(q,n),$$

$$T_\nu=T_\nu(\alpha)=\sum_{1\leqslant\mu\leqslant P}e(P_\nu(\mu)\alpha),$$

$$I_\nu=I_\nu(\alpha)=\int_0^P e(\beta\alpha_\nu v^k)\mathrm{d}v,$$

这里 $a_\nu$ 为 $P_\nu(h)$ 的首项系数.

$N$ 是所要表示的整数. 我们可以定义一个常数 $c$, 使得

$$\max_{1\leqslant\nu\leqslant s}N_\nu\leqslant cN^{\frac{1}{k}}.$$

而 $P$ 是一个满足条件

$$cN^{\frac{1}{k}}\leqslant P=O(N^{\frac{1}{k}})$$

的数.

## 3. 关于指数和的引理

**引理 3.1** 如果 $Q(h)$ 是一个整系数多项式, $(l,q)=1$, 则

$$\sum_{h=1}^{q}e\left(\frac{l}{q}Q(h)\right)=O(q^{1-\frac{1}{k}+\varepsilon}),$$

这里 $O$ 常数仅依赖于 $\varepsilon$ 和 $Q(h)$ 的系数 (见 Hua[5]).

**引理 3.2** 设 $k>20,N$ 是一个充分大的整数. 于是, 我们可以取 $P,H$(仅依赖于 $k$), 使得

$$cN^{\frac{1}{k}}\leqslant P=O(N^{\frac{1}{k}}),\quad 0<H<9k^3\log k,$$

$$\int_0^1|S|^H\mathrm{d}\alpha=O(P^{H-k+\frac{1}{20}}),$$

其中

$$S=\sum_{x=1}^{P}e(\alpha Q(x)),$$

而 $Q(x)$ 是一个 $k$ 次整值多项式.

这是 Vinogradov[3] 中的引理 $K$ 的稍加推广的形式.

**引理 3.3** 如果 $\alpha_0,\alpha_1,\cdots,\alpha_k$ 为实数, $k>20$, 而

$$\left|\alpha_0-\frac{l}{q}\right|<\frac{1}{q^2},\quad (l,q)=1,$$

$$f(x)=\alpha_0x^k+\cdots+\alpha_k,$$

则当 $P^b<q\leqslant P^{k-b}$ 时, 有

$$\sum_{x=R+1}^{R+P}e(f(x))=O(P^{1-\frac{1}{18}k^{-3}(\log k)^{-1}}).$$

见 Vinogradov[3].

## 4. Farey 分拆

我们按通常的方式, 将区间 $0\leqslant\alpha\leqslant1$ 分拆成属于所有有理点 $\frac{l}{p}(1\leqslant q\leqslant P^{k-b},0\leqslant l<q,(l,q)=1)$的 Farey 弧. 我们再将这些弧分成优弧 $M(1\leqslant q\leqslant P^b)$ 和劣弧 $m(P^b<q\leqslant P^{k-b})$. 在每一种情形里, 弧都有形式

$$\alpha=\frac{l}{q}+\beta,\quad -\frac{\theta_1}{qP^{k-b}}\leqslant\beta\leqslant\frac{\theta_2}{qP^{k-b}},\quad \frac{1}{2}\leqslant\theta_1\leqslant1,\quad \frac{1}{2}\leqslant\theta_2\leqslant1.$$

## 5. 关于优弧的引理

**引理 5.1**

$$S_{\rho,\nu}=O(q^{1-\frac{1}{k}}).$$

**证明** 设 $d$ 为 $P_\nu(h)$ 系数的最小公分母. 由连接数 $q_\nu^*$ 的定义知, 对于某个整数 $d_1$ 有 $qd=q_\nu^*d_1$, 因而,

$$S_{\rho,\nu}=\sum_{h=1}^{q_\nu^*}e\left(\frac{ldP_\nu(h)}{q_\nu^*d_1}\right)=\frac{1}{d_1}\sum_{h=1}^{q_\nu^*d_1}e\left(\frac{ldP_\nu(h)}{q_\nu^*d_1}\right).$$

因为 $dP_\nu(h)$ 是一个整系数多项式而 $d\leqslant k!$, 所以, 由引理 3.1 可得

$$S_{\rho,\nu}=O((q_\nu^*d_1)^{1-\frac{1}{k}}d_1^{-1})=O(q^{1-\frac{1}{k}}).$$

**引理 5.2** 当 $s>2k$ 时, $\mathcal{S}=\mathcal{S}(n)$ 绝对收敛.

**证明** 由引理 5.1 知

$$\left|\sum_\rho\left(\prod\frac{S_{\rho,\nu}}{q_\nu^*}\right)\rho^{-n}\right|\leqslant q\max_\rho\prod\left|\frac{S_{\rho,\nu}}{q_\nu^*}\right|=O(q^{-1-\frac{1}{k}}),$$

由此可得本引理.

**引理 5.3**

$$I_\nu = O(\min(P, |\beta|^{-\frac{1}{k}})).$$

见 Heilbronn[1] 中的 (13) 式.

**引理 5.4** 在 $M$ 上, 我们有

$$T_\nu = \frac{S_{\rho,\nu}}{q_\nu^*} I_\nu + O(P^b).$$

见 Heilbronn[1] 中的引理 4, Landau[3].

**引理 5.5** 如果 $|A_\nu - B_\nu| \leqslant C$ 且 $|B_\nu| \leqslant D$, 则有

$$\left|\prod_{\nu=1}^{t} A_\nu - \prod_{\nu=1}^{t} B_\nu\right| \leqslant K(t)(C^t + CD^{t-1}).$$

**证明** $t = 1$ 时, 引理是显然的. 用归纳法可得到一般的情形.

**引理 5.6** 如果 $s > 2k+1$, 则有

$$\sum_M \int_M \left|\prod T_\nu - \prod \frac{S_{\rho,\nu}}{q_\nu^*} I_\nu\right| \mathrm{d}\alpha = O(P^{s-k-1+b}).$$

由引理 5.5 和文献 [1] 中的引理 5 可得.

**引理 5.7** 如果 $0 < N \leqslant P^k$, 则

$$\int_{-\infty}^{\infty} \mathrm{e}^{-2\pi\mathrm{i}N\beta} \prod I_\nu \mathrm{d}\beta = \frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)} \prod a_\nu^{-\frac{1}{k}} N^{\frac{s}{k}-1}.$$

见 Landau[3].

**引理 5.8** 如果 $0 < N \leqslant P^k$, 则

$$\int_M \mathrm{e}^{-2\pi\mathrm{i}N\beta} \prod I_\nu \mathrm{d}\beta = \frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)} \prod a_\nu^{-\frac{1}{k}} N^{\frac{s}{k}-1} + O(P^{s-k-b(\frac{s}{k}-1)} q^{\frac{s}{k}-1}).$$

见 Heilbronn[1] 中的引理 7.

**引理 5.9** 如果 $0 < N \leqslant P^k$, 则

$$\sum_M \int_M \mathrm{e}^{-2\pi\mathrm{i}N\alpha} \prod T_\nu \mathrm{d}\alpha = \prod a_\nu^{-\frac{1}{k}} \frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)} \mathcal{S}(N) N^{\frac{s}{k}-1}$$

$$+O(P^{s-k-(1-b)}).$$

**证明** 由引理 5.6, 上式的左端为

$$O(P^{s-k-1+b})+\sum_{M}\left(\prod\frac{S_{\rho,\nu}}{q_\nu^*}\right)\int_{M}\mathrm{e}^{-2\pi\mathrm{i}N\alpha}\prod I_\nu\mathrm{d}\alpha$$

$$=O(P^{s-k-1+b})+\frac{\Gamma^s\left(1+\dfrac{1}{k}\right)}{\Gamma\left(\dfrac{s}{k}\right)}\prod a_\nu^{-\frac{1}{k}}N^{\frac{s}{k}-1}$$

$$\times\sum_{M}\prod\frac{S_{\rho,\nu}}{q_\nu^*}\mathrm{e}^{-2\pi\mathrm{i}N\cdot\frac{a}{q}}+O\left(\sum_{M}q^{-\frac{s}{k}}P^{s-k-b(\frac{s}{k}-1)}q^{\frac{s}{k}-1}\right)$$

$$=O(P^{s-k-1+b})+\frac{\Gamma^s\left(1+\dfrac{1}{k}\right)}{\Gamma\left(\dfrac{s}{k}\right)}\prod a_\nu^{-\frac{1}{k}}N^{\frac{s}{k}-1}$$

$$\times\left(\mathcal{S}+\sum_{q>P^b}O(q^{1-\frac{s}{k}})\right)+O(P^{s-k-b(\frac{s}{k}-1)})\sum_{M}q^{-1}$$

$$=O(P^{s-k-1+b})+\prod a_\nu^{-\frac{1}{k}}\frac{\Gamma^s\left(1+\dfrac{1}{k}\right)}{\Gamma\left(\dfrac{s}{k}\right)}\mathcal{S}N^{\frac{s}{k}-1}+O(P^{s-k-b(\frac{s}{k}-2)}).$$

## 6. 关于劣弧的引理

**引理 6.1** 如果 $s>10k^3\log k$ 且 $k>20$, 则有

$$\sum_{m}\int_{m}\prod_{\nu=1}^{s}T_\nu\mathrm{e}^{-2\pi\mathrm{i}N\alpha}\mathrm{d}\alpha=O(P^{s-k-(1-b)}).$$

**证明** 选取 $H$ 和 $P$ 满足引理 3.2 的要求. 因为几何平均小于算术平均, 所以

$$\int_0^1\prod_{\nu=1}^{H}|T_\nu|\mathrm{d}\alpha\leqslant\frac{1}{H}\sum_{\nu=1}^{H}\left(\int_0^1|T_\nu|^H\mathrm{d}\alpha\right)=O(P^{H-k+\frac{1}{20}}).$$

因此, 用引理 3.3 可得

$$\sum_{m}\int_{m}\prod_{\nu=1}^{H}|T_\nu|\mathrm{d}\alpha=O\left(\max_{m}\prod_{\nu=H+1}^{s}|T_\nu|\int_0^1\prod_{\nu=1}^{H}|T_\nu|\mathrm{d}\alpha\right)$$
$$=O(P^{(1-\frac{1}{18}k^{-3}(\log k)^{-1})(s-H)+H-k+\frac{1}{20}})$$

$$= O(P^{s-k-(1-b)}).$$

**定理 1** 设 $r(N)$ 为丢番图方程

$$N = P_1(x_1) + \cdots + P_s(x_s), \quad x_\nu \geqslant 0$$

的解数. 当 $k > 20, s > 10k^3\log k$ 时, 我们有

$$r(N) = \prod_{\nu=1}^{s} a_\nu^{-\frac{1}{k}} \frac{\Gamma^s\left(1+\dfrac{1}{k}\right)}{\Gamma\left(\dfrac{s}{k}\right)} \mathcal{S}(N) N^{\frac{s}{k}-1} + O(P^{s-k-1+b}).$$

由引理 5.9 和 6.1 可得本定理.

# 7. 关于同余式和奇异级数的引理

下面的记号将用于本文余下的部分:

$d_\nu$ 为 $P_\nu(h)$ 所有系数的最小公分母, $d_\nu P_\nu(h) = \phi_\nu(h)$.

$\theta_\nu$ 为使得

$$\phi'_\nu(h) \equiv 0(\mathrm{mod} p^{\theta_\nu})$$

对于所有 $h$ 都成立的 $p$ 的最高次幂.

$$P^*_\nu(h) = p^{-\theta_\nu}\phi'_\nu(h).$$

$M(n) = M(P_1, \cdots, P_s, m, n)$ 为同余式

$$n \equiv P_1(h_1) + \cdots + P_s(h_s)(\mathrm{mod} m),$$
$$0 \leqslant h_\nu \leqslant m^*_\nu, \quad \nu = 1, 2, \cdots, s \tag{7.1}$$

的解数.

当 $m = p^l$ 时, $N(p^l, n) = N(P_1, \cdots, P_s; p^l, n)$ 表示 (7.1) 式中这样的解的个数, 其中 $P^*_1(h_1), \cdots, P^*_s(h_s)$ 至少有一个与 $p$ 互素.

如果 $P_1, \cdots, P_s$ 为相同的多项式, 则令

$$M(s \cdot P, m, n) = M(P_1, \cdots, P_s, m, n),$$
$$N(s \cdot P, p^l, n) = N(P_1, \cdots, P_s, p^l, n).$$

$\delta$ 为满足 $p^\delta \leqslant k-1$ 的最大整数.

如果我们用 $p^*_\nu = p^{1+t_\nu}$ 来定义 $t_\nu$, 则 $d_\nu = p^{t_\nu} d'_\nu, (d'_\nu, p) = 1$,

$$\gamma_\nu = \begin{cases} \theta_\nu + 2 - t_\nu + \delta, & \text{当 } p = 2 \text{ 时}, \\ \theta_\nu + 1 - t_\nu + \delta, & \text{当 } p \neq 2 \text{ 时}. \end{cases}$$

$$\gamma=\max(\gamma_1,\cdots,\gamma_s).$$

**引理 7.1** 如果 $(m^{(1)},m^{(2)})=1$, 则有

$$M(m^{(1)})M(m^{(2)})=M(m^{(1)}m^{(2)}).$$

**引理 7.2**

$$\sum_{q|m}A(q)=\frac{m}{\prod m_\nu^*}M(m).$$

**引理 7.3** 如果 $(m^{(1)},m^{(2)})=1$, 则有

$$\sum_{q|m^{(1)}m^{(2)}}A(q)=\sum_{q|m^{(1)}}A(q)\sum_{q|m^{(2)}}A(q).$$

以上三个引理可由 Landau[4] 中的方法证得.

**引理 7.4** 如果 $Q(h)$ 是一个 $k$ 次剩余多项式 $(\text{mod}p^\alpha)$, 而 $Q'(h)$ 是一个剩余多项式 $(\text{mod}p^\beta)$, 则有

$$p^{\alpha-\beta}\leqslant k.$$

**证明** (1) 首先, 我们考虑特殊情形

$$Q(h)=Q_r(h)=h(h-1)\cdots(h-r+1).$$

此时

$$\alpha=\sum_{l=1}^{\infty}\left[\frac{r}{p^l}\right].$$

因为 $|Q_r'(i)|=i!(r-i-1)!$, 所以, 我们有

$$\beta=\min_{0\leqslant i\leqslant r}\left\{\sum_{l=1}^{\infty}\left(\left[\frac{r-1-i}{p^l}\right]+\left[\frac{i}{p^l}\right]\right)\right\}.$$

如果 $p^\sigma|r$ 且 $p^{\sigma+1}\nmid r$, 则有

$$\alpha-\sum_{l=1}^{\infty}\left[\frac{r-1}{p^l}\right]=\sigma$$

和

$$\sum_{l=1}^{\infty}\left[\frac{r-1}{p^l}\right]-\sum_{l=1}^{\infty}\left(\left[\frac{r-1-i}{p^l}\right]+\left[\frac{i}{p^l}\right]\right)\leqslant\delta_1-\sigma,$$

其中 $\delta_1$ 为满足 $p^{\delta_1}\leqslant r$ 的最大整数. 因此, 引理对于 $Q_r(h)$ 成立.

(2) 因为 $Q(h)$ 可以写成

$$Q(h)=\sum_{r=1}^{k}a_rQ_r(h),$$

而 $a_rQ_r(h)(r=1,2,\cdots,k)$ 为剩余多项式 $(\bmod p^\alpha)$, 所以, 由情形 (1) 可得引理.

**引理 7.5** 如果 $l\geqslant\gamma_\nu+1$ 且 $h=y+p^{l+t_\nu-\theta_\nu-1}z$, 则有

$$P_\nu(h)\equiv P_\nu(y)+zp^{l-1}P_\nu^*(y)(\bmod p^l)$$

以及

$$P_\nu^*(h)\equiv P_\nu^*(y)(\bmod p).$$

**证明** 由 Taylor 展开可得

$$\begin{aligned}\phi_\nu(h)\equiv\ &\phi_\nu(y)+zp^{l+t_\nu-\theta_\nu-1}\phi_\nu'(y)\\&+\frac{1}{2!}z^2p^{2(l+t_\nu-\theta_\nu-1)}\phi_\nu''(y)\\&+\frac{1}{3!}z^3p^{3(l+t_\nu-\theta_\nu-1)}\phi_\nu'''(y)+\cdots.\end{aligned}$$

(1) $p\neq2$. 因为 $\phi_\nu''(y)$ 是一个剩余多项式 $(\bmod p^{\theta_\nu-\delta})$, 所以

$$\phi_\nu(h)\equiv\phi_\nu(y)+zp^{l+t_\nu-\theta_\nu-1}\phi_\nu'(y)(\bmod p^{l+t_\nu})$$

(注意当 $i\geqslant z$ 时, 有

$$p^{i(l+t_\nu-\theta_\nu-1)}\frac{\phi_\nu^{(i)}(y)}{i!}\equiv0(\bmod p^{l+t_\nu})).$$

(2) $p=2$. 此时, $\frac{1}{2}\phi_\nu''(y)$ 是一个剩余多项式 $(\bmod p^{\theta_\nu-\delta-1})$. 用情形 (1) 中的讨论可得引理.

我们用相同的讨论可得到第二个结论.

**引理 7.6** 如果 $l\geqslant\gamma_\nu+1$, 则有

$$N(p^l)=p^{s-1}N(p^{l-1}).$$

**证明** 在 (7.1) 式中, 令

$$h_\nu=y_\nu+p^{l+t_\nu-\theta_\nu-1}z_\nu,$$

其中 $0\leqslant y_\nu<p^{l+t_\nu-\theta_\nu-1},0\leqslant z_\nu<p^{\theta_\nu+1}$, 而 $p$ 不能整除每一个 $P_\nu^*(y_\nu)$. 我们可得

$$\sum_{\nu=1}^sP_\nu(y_\nu)+p^{l-1}\sum_{\nu=1}^sz_\nu P_\nu^*(y_\nu)\equiv n(\bmod p^l)\begin{cases}0\leqslant y_\nu<p^{l+t_\nu-\theta_\nu-1},\\0\leqslant z_\nu<p^{\theta_\nu+1}.\end{cases}$$

这个同余式的每一个解都对应于下面两个同余式的一个解

$$\sum_{\nu=1}^sP_\nu(y_\nu)\equiv n(\bmod p^{l-1}),\quad 0\leqslant y_\nu<p^{l+t_\nu-\theta_\nu-1},\quad p\nmid\text{每一个}P_\nu^*(y_\nu);\qquad(7.6.1)$$

$$\sum_{\nu=1}^{s} z_\nu P_\nu^*(y_\nu) \equiv p^{-(l-1)}\left(n-\sum_{\nu=1}^{s} P_\nu(y_\nu)\right)(\mathrm{mod}p), \quad 0 \leqslant z_\nu < p^{\theta_\nu+1}, \tag{7.6.2}$$

反之亦然.

接下来我们将证明前者有 $\prod p^{-\theta_\nu} N(p^{l-1})$ 个解, 而后者有 $p^{-1}\prod p^{\theta_\nu+1}$ 个解.

由引理 7.5 知, 当 $x_\nu \equiv y_\nu(\mathrm{mod}p^{l+t_\nu-\theta_\nu-1})$ 时, 我们有 $P_\nu(x_\nu) \equiv P_\nu(y_\nu)(\mathrm{mod}p^{l-1})$. 因此, (7.6.1) 式的每个解都给出

$$\sum_{\nu=1}^{s} P_\nu(y_\nu) \equiv n(\mathrm{mod}p^{l-1}), \quad 0 \leqslant y_\nu < p^{l+t_\nu-1}, \quad p\nmid 每一个P_\nu^*(y_\nu)的\prod p^{\theta_\nu}个解.$$

因为 $p$ 不能整除每一个 $P_\nu^*(y_\nu)$, 我们可设 $p \nmid P_1^*(y_1)$. 于是, 在 (7.6.2) 式中可以 $(\mathrm{mod}p^{\theta_\nu+1})$ 任意地选取 $z_\nu(\nu=2,3,\cdots,s)$, 而 $z_1$ 是 $(\mathrm{mod}p)$ 唯一确定的. 因而, 对于任一组 $z_\nu(\mathrm{mod}p^{\theta_\nu+1})(\nu=2,3,\cdots,s)$, 有 $p^{\theta_1}$ 个解 $z_1$ 满足 $0 \leqslant z_1 < p^{\theta_1+1}$. 我们可知, (7.6.2) 式有 $p^{-1}\prod_{\nu=1}^{s} p^{\theta_\nu+1}$ 个解.

作为上面引理的推论, 我们有

**引理 7.7** 如果 $l \geqslant \gamma$, 则有

$$N(p^l) = p^{(l-\gamma)(s-1)} N(p^\gamma).$$

**引理 7.8** 如果对于所有的整数 $n$, 有 $M(P_1,\cdots,P_{s-1},p^l,n) > 0$, 则

$$N(P_1,\cdots,P_{s-1},P_s,p^l,n) > 0$$

对于所有的整数 $n$ 成立.

**证明** 因为 $P_s^*(h)$ 不是恒等地同余 $0(\mathrm{mod}p)$, 则有整数 $h_s$ 使得 $p \nmid P_s^*(h_s), 0 \leqslant h < p^{l+t_s}$. 由假设的条件, 我们可见方程

$$\sum_{\nu=1}^{s-1} P_\nu(h_\nu) \equiv n - P_s(h_s)(\mathrm{mod}p^l)$$

有至少一个解, 因此, 引理成立.

令 H 为假设: 对于所有的素数 $p$ 和所有的整数 $n$, 有

$$N(P_1,\cdots,P_{s_0},n,p^\gamma) > 0.$$

**引理 7.9** 如果假设 H 成立且 $s \geqslant \max(s_0,2k)$, 则有

$$\mathcal{S}(n) \geqslant D_1 > 0,$$

这里 $D_1$ 为依赖于 $P_\nu(h)(\nu=1,2,\cdots,s)$ 的系数的正常数, 下面出现的 $D_2,D_3,D_4$ 亦然.

**证明** 由引理 7.2 知

$$\sum_{q|p^l} A(q) = \frac{p^l}{\prod p^{l+t_\nu}} M(p^l).$$

再由引理 7.7,

$$\sum_{q|p^l} A(q) \geqslant p^{-l(s-1)-\sum t_\nu} N(p^l) \geqslant p^{-\gamma(s-1)-\sum t_\nu}, \tag{7.9.1}$$

这里的下界已与 $l$ 无关. 由引理 5.1 可得

$$\sum_{q|p^l} A(q) = 1 + \sum_{\lambda=1}^{l} A(p^\lambda) > 1 - D_2 \sum_{\lambda=1}^{\infty} p^{-\frac{\lambda}{b}} = 1 - \frac{D_2}{(p^{\frac{1}{b}} - 1)}.$$

如果 $p > D_3 = (D_2+1)^b$, 则

$$\prod_{D_3 < p \leqslant p_l} \sum_{q|p^l} A(q) > \prod_{D_3 < p} \left(1 - \frac{D_2}{(p^{\frac{1}{b}} - 1)}\right),$$

其中 $p_l$ 为第 $l$ 个素数. 上式的右端是收敛的. 再由 (7.9.1) 式知

$$\prod_{p \leqslant D_3} \sum_{q|p^l} A(q) > D_4,$$

这里 $D_4$ 与 $l$ 无关.

令 $l$ 趋向无穷. 由引理 7.3 可得

$$\mathcal{S}(n) \geqslant D_1 > 0.$$

因此, 我们有

**定理 2** 当假设 H 成立且 $s > \max(s_0 - 1, 10k^3 \log k)$ 时, 有

$$r_{P_1,\cdots,P_s}(n) > 0.$$

由 Hardy-Littlewood[1] 知, 当 $s_0 = 4k$ 以及 $P_1 = P_2 = \cdots = P_{4k} = x^k$ 时, 假设 H 成立. 当 $P_1 = P_2 = \cdots = P_{4k} = x^k$, 而 $P_{4k+1}, \cdots, P_{s_0}$ 为任意时, 假设 H 就更成立了. 因此, 我们有

**定理 3** 如果 $P_{4k+1}(h), \cdots, P_s(h)$ 为任意 $k$ 次整值多项式, $s > 10k^3 \log k$, 则当 $N$ 为充分大的整数时, 我们可以取正整数 $h_1, h_2, \cdots, h_s$, 使得

$$N = h_1^k + \cdots + h_{4k}^k + P_{4k+1}(h_{4k+1}) + \cdots + P_s(h_s) \quad (h_\nu \geqslant 0).$$

更一般地, 我们有

**定理 4** 如果 $a_1, a_2, \cdots, a_t$ 为 Huston[1] 中定义的容许集, $P_{t+1}(h), \cdots, P_s(h)$ 为任意整值多项式, 则当 $N$ 为充分大的整数且 $s > 10k^3\log k$ 时, 丢番图方程

$$N = a_1h_1^k + \cdots + a_th_t^k + P_{t+1}(h_{t+1}) + \cdots + P_s(h_s)$$

有正整数解.

在本文的余下部分中, $\theta_\nu, t_\nu, \phi_\nu, \cdots$ 中的下标 $\nu$ 将忽略.

## 8. 关于 $\theta$ 的引理

**引理 8.1** 如果 $p > k$, 则有 $\theta = 0$ 和 $t = 0$.

**引理 8.2** 如果 $p \leqslant k$, 则有

$$p^\theta \leqslant k2^{k-1}.$$

**证明** 令

$$\phi(h) = c_0h^k + \cdots + c_{k-1}h.$$

于是

$$p \nmid (c_0, \cdots, c_{k-1}).$$

令 $\delta_1$ 为使

$$p^{\delta_1} | (kc_0, (k-1)c_1, \cdots, 2c_{k-2}, c_{k-1})$$

成立的 $p$ 的最高次幂. 而令 $\delta_2$ 为 $p$ 的最高次幂, 使得存在一个 $k-1$ 次的剩余多项式 $(\mathrm{mod} p^{\delta_2})$, 它至少有一个系数不能被 $p$ 整除. 于是, 有

$$\theta \leqslant \delta_1 + \delta_2.$$

因为 $p \nmid (c_0, c_1, \cdots, c_{k-1})$, 所以 $p^{\delta_1}$ 必定整除 $1, 2, \cdots, k$ 中的一个, 因而 $p^{\delta_1} \leqslant k$. 由

$$\delta_2 \leqslant \sum_{l=1}^{\infty} \left[\frac{k-1}{p^l}\right] \leqslant \frac{k-1}{p-1}$$

可得

$$p^{\delta_2} \leqslant p^{\frac{k-1}{p-1}} = \mathrm{e}^{\frac{(k-1)\log p}{p-1}}.$$

当 $x$ 跑遍所有 $\geqslant 2$ 的整数时, $\log x/(x-1)$ 在 $x = 2$ 处取最大值. 因此

$$p^\theta \leqslant p^{\delta_1+\delta_2} \leqslant k2^{k-1}.$$

因此, 我们有

**引理 8.3** 如果 $p < k, k \geqslant 4$, 则有

$$p^{\gamma} \leqslant k^3 2^{k-1}.$$

## 9. Tarry 问题与关于奇多项式的华林问题之间的关系

令 $P(h)$ 为一个奇多项式, 则

$$P(h) = b_0 Q_{2l+1}(h) + b_1 Q_{2l-1}(h) + \cdots + b_l Q_1(h),$$

其中

$$Q_{2\mu+1}(h) = \frac{h(h^2-1)\cdots(h^2-\mu^2)}{(2\mu+1)!},$$

$b_i$ 为整数, 而

$$(b_0, b_1, \cdots, b_l) = 1.$$

参见 Hua[3] 中的引理 2 和 4.

**引理 9.1** 如果 $s \geqslant \frac{1}{3}(2^{k+1}-1)$, 则

$$N(s \cdot P, p^l, n) > 0.$$

见 Hua[3] 中的引理 40.

在第 9 和 10 节中将证明, 如果对于确定的 $k = k_0$, 我们可以找到 Tarry 问题的一个特殊解 (非平凡), 则由此我们可以对于所有的 $k \geqslant k_0$ 推出 $G\{P(h)\}$ 的一个上界.

我们设这个特殊解为 $a_1, \cdots, a_{j_0}; b_1, \cdots, b_{j_0}$, 即

$$\begin{cases} a_1^h + \cdots + a_{j_0}^h = b_1^h + \cdots + b_{j_0}^h \quad (1 \leqslant h \leqslant k_0 - 2), \\ a_1^{k_0-1} + \cdots + a_{j_0}^{k_0-1} \neq b_1^{k_0-1} + \cdots + b_{j_0}^{k_0-1}. \end{cases} \tag{9.1}$$

令

$$a_1^{k_0-1} + \cdots + a_{j_0}^{k_0-1} - b_1^{k_0-1} - \cdots - b_{j_0}^{k_0-1} = X(a, b, k_0),$$

而令 $X$ 的最大素因子为 $p$. 对于 (9.1) 式的每一个解, 我们都有一个对应的数 $q = \max(j_0, p)$. 诸 $q$ 的最小者记为 $T(k_0)$.

**引理 9.2** 设 $k \geqslant k_0$,

$$k - 1 = l(k_0 - 1) + m, \quad l > 0, \quad 0 \leqslant m < k_0 - 1, \quad j \geqslant 2^{m+l-1} j_0^l,$$

则存在一组整数 $x_1, \cdots, x_j; y_1, \cdots, y_j$, 使得

$$x_1^h + \cdots + x_j^h = y_1^h + \cdots + y_j^h \quad (1 \leqslant h \leqslant k-2),$$
$$x_1^{k-1} + \cdots + x_j^{k-1} \neq y_1^{k-1} + \cdots + y_j^{k-1},$$

且

$$X(k) + x_1^{k-1} + \cdots + x_j^{k-1} - y_1^{k-1} - \cdots - y_j^{k-1}$$

的最大素因子不超过 $k$ 和 $\boldsymbol{p}$ 的最大者.

**证明** 用 Maitland Wright[3] 中的讨论, 我们可以构造一个多项式

$$f_0(y) = (y-1)^{k_0-1} h_0(y) = \sum_{i=1}^{j_0} y^{a_i} - \sum_{i=1}^{j_0} y^{b_i},$$

且容易验证

$$\left\{ \left( y \frac{\mathrm{d}}{\mathrm{d}y} \right)^{k_0-1} f_0(y) \right\}_{y=1} = (k_0-1)! h_0(1) = X(k_0).$$

再构造

$$f(y) = (y-1)^m (f_0(y))^l = (y-1)^{k-1} (k_0(y))^l.$$

则 $f(y)$ 包含至多 $2^m(2j_0^l)$ 个形如 $\pm y^a$ 的项. 进一步地, 有

$$X(k) = \left\{ \left( y \frac{\mathrm{d}}{\mathrm{d}y} \right)^{k-1} f(y) \right\}_{y=1} = (k-1)!(h_0(1))^l.$$

因而, 引理得证.

**引理 9.3** 如果 $p > k$ 且 $s \geqslant \max\left(\boldsymbol{p}, 2^{m+l-1} j_0^l, \frac{1}{3}(2^{k_0+1}-1)\right)$, 则对于所有的奇多项式 $P(h)$, 有

$$N(s \cdot P, p^\gamma, n) > 0$$

(实际上, 这里的 $\gamma = 1$).

注意当 $k$ 增长时, 只有 $2^{m+l-1} j_0^l$ 增长, 而其他项保持不变.

**证明** (1) 当 $p \leqslant \max(\boldsymbol{p}, k)$ 时, 结论显然.

(2) 当 $p > \max(\boldsymbol{p}, k)$ 时 (此时 $\gamma = 1$), $p \nmid X(k)$. 如果 $p \nmid a$($a$ 为 $P(h)$ 的首项系数, 它不必为整数, 它的分母与 $p$ 互素), 则对于任一个整数 $n$, 我们总可以取 $x_i, y_i$ 和 $x$, 使得 $j \leqslant 2^{m+l-1} j_0^l$ 且

$$\sum_{i=1}^{j} (P(x+x_i) - P(x+y_i)) = aX(k)x + Y(k) \equiv n (\mathrm{mod} p).$$

如果 $p|a$, 则 $P(h)\equiv Q(h)(\bmod p)$, 这里 $Q(h)$ 为次数低于 $P(h)$ 的多项式. 当 $Q(h)$ 的次数超过 $k_0$ 时, 我们可以对它用上面的讨论. 如果 $Q(h)$ 的次数不高于 $k_0$, 则由引理 9.1 知, 对于任一个整数 $n$ 和 $s\geqslant\frac{1}{3}(2^{k_0+1}-1)$, 同余式

$$\sum_{\nu=1}^{s}Q(h_\nu)\equiv n(\bmod p)$$

有解. 因此, 引理得证.

**引理 9.4** 对于任给的 $\varepsilon>0$, 当 $k\to\infty$ 时, 有

$$2^{m+l-1}j_0^l=O(2^{\varepsilon k}).$$

**证明** 如果 $k_0$ 很大, 则由 Maitland Wright[4] 中的结果知

$$\begin{aligned}2^{m+l-1}j_0^l&\leqslant 2^{m+l-1}\left(\frac{7k_0^2(k_0-11)^2}{72}+56\right)^l\\&\leqslant 2^{m+l-1}k_0^{4l}\\&\leqslant 2^{k_0-1-\frac{(k-1)}{k_0-1}-1}k_0^{\frac{4(k-1)}{k_0-1}}\\&\leqslant 2^{k_0-2+\frac{(k-1)}{k_0-1}\left(-1+\frac{4\log k_0}{\log 2}\right)}.\end{aligned}$$

因为

$$\lim_{k_0\to\infty}\frac{1}{k_0-1}\left(-1+\frac{4\log k_0}{\log 2}\right)=0,$$

所以, 对于任给的 $\varepsilon>0$, 总是一个 $k_0$ 使得

$$\frac{1}{k_0-1}\left(-1+\frac{4\log k_0}{\log 2}\right)<\varepsilon,$$

由此可得引理.

**引理 9.5** 如果 $k\geqslant 10, p>k, s\geqslant 2^{\frac{1}{2}(k-1)+7}$, 而 $P(h)$ 为奇多项式, 则有

$$N(s\cdot P,p^\gamma,n)>0.$$

**证明** 因为

$$\begin{aligned}&1^h+5^h+10^h+24^h+28^h+42^h+47^h+51^h\\=&2^h+3^h+12^h+21^h+31^h+40^h+49^h+50^h\quad(1\leqslant h\leqslant 7)\end{aligned}$$

和

$$\begin{aligned}&1^8+5^8+10^8+24^8-28^8+42^8+47^8+51^8\\&-2^8-3^8-12^8-21^8-31^8-40^8-49^8-50^8\end{aligned}$$

$$=2^{11}\cdot 3^3\cdot 5^2\cdot 7^2\cdot 11\cdot 13,$$

所以, 有

$$k_0=9,\quad j_0=8,\quad \boldsymbol{p}=13.$$

这里

$$\max\left(\boldsymbol{p},\frac{1}{3}2^{k_0+1}\right)=341$$

以及

$$2^{m+j-1}j_0^l=2^{m+4l-1}\leqslant 2^{k_0-1-\frac{4(k-1)}{k_0-1}-1}=2^{\frac{1}{2}(k-1)+7}.$$

由引理 9.3 可得结论.

用定理 2 和引理 9.1, 我们可得

**定理 5** 如果 $k>20$, 则每个充分大的整数可以表作 $\frac{1}{3}(2^{k+1}-1)$ 个数之和, 其中每个数均为 $k$ 次奇多项式 $P(h)(h\geqslant 0)$ 的值.

**定理 6** 如果 $P(h)$ 的首项系数为 $a/k!,(a,k!)=1$, 则

$$G\{P(h)\}=O(2^{\varepsilon k}).$$

由引理 9.4 并注意 $\gamma\leqslant\delta+2$, 即可得本定理.

## 10. 关于一般多项式的引理

令 $K(2l)$ 为最小的 $s$, 使得同余方程组

$$x_1^{2\nu}+\cdots+x_s^{2\nu}\equiv 0(\mathrm{mod}p),\quad p\nmid x_1,\quad \nu=1,\cdots,l$$

有解. 我们设 $p>k$ 和 $2l\leqslant k$.

**引理 10.1** 如果有

$$x_1^{\mu}+\cdots+x_{s_1}^{\mu}\equiv 0(\mathrm{mod}p),\quad p\nmid x_1$$

和

$$y_1^{\nu}+\cdots+y_{s_2}^{\nu}\equiv 0(\mathrm{mod}p),\quad p\nmid y_1,$$

则

$$\sum_{t_2=1}^{s_2}\sum_{t_1=1}^{s_1}(x_{t_1}y_{t_2})^{\nu}\equiv 0(\mathrm{mod}p)$$

以及

$$\sum_{t_2=1}^{s_2}\sum_{t_1=1}^{s_1}(x_{t_1}y_{t_2})^{\mu}\equiv 0(\mathrm{mod}p).$$

**引理 10.2**　存在一个整数 $m \leqslant 2l$ 使得 $m|p-1$, 但不存在整数 $\nu \leqslant l$ 满足

$$m|(p-1,2\nu) \text{ 和 } \frac{(p-1,2\nu)}{m}>1.$$

以上两个引理是显然的.

**引理 10.3**　当 $m$ 如引理 10.2 中选取且 $s \geqslant m(m+1)^{[\frac{2l}{m}]}$ 时, 同余方程组

$$x_1^{2\nu}+\cdots+x_s^{2\nu} \equiv 0(\bmod p), \quad p \nmid x_1, \quad \nu=1,\cdots,l \tag{10.3}$$

有解.

**证明**　因为 $m|(p-1)$, 所以, 存在一个整数 $g$ 属于 $m(\bmod p)$. 因而, 对于所有满足 $m \nmid 2\nu$ 的 $\nu$, 有

$$1^{2\nu}+g^{2\nu}+(g^2)^{2\nu}+\cdots+(g^{m-1})^{2\nu} \equiv 0(\bmod p). \tag{10.3.1}$$

而未被讨论的 $\nu$ 即为满足

$$(2\nu,p-1)=m$$

者. 由 Landau[1] 中的定理 301, 我们可取 $x_1,\cdots,x_{m+1}$, 使得

$$x_1^{2\nu}+\cdots+x_{m+1}^{2\nu} \equiv 0(\bmod p), \quad p \nmid x_1.$$

至多 $\left[\frac{2\nu}{m}\right]$ 个 $\nu$ 有此性质. 因此, 由引理 10.1, 可得本引理.

**引理 10.4**

$$K(2l) \leqslant 2l \cdot 3^l.$$

如果 $l \geqslant 22$, 则

$$K(2l)<3^l.$$

**证明**　(1) 这里

$$(m+1)^{[\frac{2l}{m}]} \leqslant (m+1)^{\frac{2l}{m}}=\mathrm{e}^{\frac{2l\log(m+1)}{m}}.$$

因为当 $x>\mathrm{e}-1$ 时, $\log(x+1)/x$ 是单调递减的, 所以, 我们有

$$(m+1)^{[\frac{2l}{m}]} \leqslant 3^l.$$

(2) 当 $m=2$ 时, 因为没有形如 (10.3.1) 式的同余式, 我们可以证明

$$K(2l)<3^l.$$

当 $m \geqslant 3$ 时, 有

$$K(2l)<m(m+1)^{[\frac{2l}{m}]} \leqslant 2l \cdot 4^{\frac{2}{3}l};$$

而当 $l \geqslant 22$ 时, 有

$$2l \cdot 4^{\frac{2}{3}l} \leqslant 3^l.$$

**引理 10.5** 如果 $s > K(2l)$, $t$ 是任意的奇数, 则有整数 $h_1, \cdots, h_s$, 使得

$$h_1^{2r} + \cdots + h_s^{2r} \equiv 0(\mathrm{mod} p), \quad l \geqslant r \geqslant 1 \tag{10.5.1}$$

以及

$$h_1^t + \cdots + h_s^t \not\equiv 0(\mathrm{mod} p). \tag{10.5.2}$$

**证明** 由引理 10.4, 我们可以取 $h_1, \cdots, h_s$, 满足 (10.3) 式和

$$h_1^t + h_2^t + \cdots + h_s^t \not\equiv (-h_1)^t + h_2^t + \cdots + h_s^t (\mathrm{mod} p),$$

结论立得.

每个没有常数项的整值多项式 $R(h)$ 可以写成

$$R(h) = \frac{1}{2}(hR_1(h) + R_2(h)),$$

这里 $R_1(h), R_2(h)$ 为两个奇多项式. 显然, $hR_1(h), R_2(h)$ 都是整值多项式. 令 $hR_1(h), R_2(h)$ 的次数分别为 $2t_1$ 和 $2t_2+1$. 我们可记

$$R_2(h) = \sum_{\nu=1}^{t_2} c_\nu Q_{2\nu+1}(h),$$

其中 $c_\nu$ 都是整数.

**引理 10.6** 如果没有整数 $a$ 使得 $P(h) \equiv a(\mathrm{mod} p)$ 恒等地成立, 则存在一个整数 $q$, 使得由 $R(h) = P(h+q)$ 导出的 $R_2(h)$ 的系数 $c_\nu$ 满足

$$p \nmid (c_1, \cdots, c_{t_2}) \quad (p \neq 2).$$

**证明** 显然,

$$P(h) - R(-h) = R_2(h).$$

假设结论不对. 因为 $R_2(0) = 0$, 所以, 对于所有的 $h$ 和 $q$, 我们有

$$P(h+q) - P(-h+q) \equiv 0(\mathrm{mod} p).$$

特别地, 我们取 $h = q$, 则对于所有的 $h$,

$$P(2h) \equiv 0(\mathrm{mod} p),$$

但这与我们的假设相矛盾.

令 $\Gamma\{P(h),p\}$ 为最小的正整数 $s$, 使得对于所有的 $n$, 同余式

$$\sum_{\nu=1}^{s} P(h_\nu) \equiv n(\mathrm{mod} p^\gamma)$$

总有解.

**引理 10.7** 如果 $p > k$, 则存在一个次数不超过 $2t_1+1$ 的奇多项式 $Q(h) \not\equiv 0(\mathrm{mod} p)$, 使得当

$$s \geqslant K(2t_1)\Gamma\{Q(h),p\}$$

时, 对于任一个整数 $n$, 同余式

$$\sum_{\nu=1}^{s} P(h_\nu) \equiv n(\mathrm{mod} p)$$

总有解.

**证明** 由引理 10.6 知, 存在一个整数 $q$ 使得

$$R_2(h) \not\equiv 0(\mathrm{mod} p).$$

于是, 我们可以定义整数 $\tau$ 使得

$$p|(c_{t_2},\cdots,c_{t_2-\tau+1}), \quad p\nmid c_{t_2-\tau}, \quad 0 \leqslant \tau < t_2.$$

令 $h_1,\cdots,h_{s_1}(s_1 = K(2t_1))$ 满足

$$h_1^{2\nu}+\cdots+h_s^{2\nu} \equiv 0(\mathrm{mod} p), \quad \nu = 1,\cdots,t_1$$

以及

$$h_1^{2(t_2-\tau)+1}+\cdots+h_s^{2(t_2-\tau)+1} \not\equiv 0(\mathrm{mod} p). \tag{10.7.1}$$

我们来看

$$\Psi(h) = \sum_{\nu=1}^{s_1} R(h_\nu h)(\mathrm{mod} p).$$

这里 $\Psi(h)$ 为一个奇多项式. 由 (10.7.1) 式知

$$\Psi(h) \not\equiv 0(\mathrm{mod} p).$$

由此立得引理.

由引理 8.3,9.3,9.4,10.4 和 10.7, 我们可得

**引理 10.8** 对于任给的 $\varepsilon > 0$,

$$\Gamma\{P(h),p\} = O(3^{k(\frac{1}{2}+\varepsilon)})$$

对于所有的 $p > k$ 成立.

**定理 7** $G\{P(h)\} = O(k^3 2^{k-1})$.

由引理 8.3,9.5,10.4 和 10.7, 我们可得

**引理 10.9** 如果 $k \geqslant 15$, 则有

$$\Gamma\{P(h), p\} \leqslant \max(k3^{[\frac{1}{3}k]}2^{\frac{1}{2}(k-1)+7}, k^3 2^{k-1})$$
$$\leqslant k3^{\frac{1}{3}k}2^{\frac{1}{2}(k-1)+7}.$$

因此, 我们有

**定理 8** 当 $k > 20$ 时, 每个充分大的整数可表为一个 $k$ 次多项式 $P(h)(h \geqslant 0)$ 的 $[k3^{\frac{1}{2}k}2^{\frac{1}{2}(k-1)+7}]$ 个值之和.

**定理 9** 如果 $P(h)$ 的首项系数为 $a/k!, (a, k!) = 1$, 则

$$G\{P(h)\} = O(3^{k(\frac{1}{2}+\varepsilon)}).$$

## 11. 一些进一步的结果

本节中, 我们将描述一些可用于特殊多项式的方法, 并简要地指出由它们得到的更多有趣的结果.

(1) 由 Heilbronn 方法, 我们可以证明, 如果整数

$$a_1, a_2, \cdots, a_s$$

中有 $4k$ 个构成 Huston 定义的一个容许集, 则当

$$s \geqslant 6k\log k + \left\{4 + 3\log\left(3 + \frac{2}{k}\right)\right\}k + 3$$

时, 对于所有充分大的整数 $n$, 方程

$$a_1 h_1^k + \cdots + a_s h_s^k = n$$

总有非负整数解. 这包含了 Dickson[1] 关于推广的华林问题的一个结果.

(2) 如果我们用 Weyl 逼近代替引理 3.2 和 3.3, 并用 Wright[2,3] 的方法, 由于

$$s \geqslant 2^{k-1}(k-2) + 5 \quad (k \geqslant 3),$$

我们能够对于多项式证明推广的 Wright 渐近公式. 由此我们可以推出如下的关于低次多项式的结果.

令 $G^*\{P(h)\}$ 为最佳的整数，使得 Waring-Kamke 问题在比例条件下可解. 这里必定不存在整数 $c$ 和 $d(d>1)$，使得

$$P(h)\equiv c(\bmod d)$$

恒等地成立. 结果概述如下.

1. 如果 $P(h)$ 为 3 次整值多项式，则有

$$G^*\{P(h)\}\leqslant 9.$$

因为去掉了系数的限制条件，所以，这个结果比 James[1] 的结果要好，可参见 James[2] 和 Hua[1].

2. $G^*\left\{\frac{1}{12}A(h^4-h^2)+Bh^2\right\}\leqslant 26\quad[(A,6B)=1]$.

3. $G^*\left\{\frac{1}{12}A(h^4-h^2)+Bh^2\right\}\leqslant 31\quad[(A,B)=1]$.

4. 如果 $P(h)$ 为 4 次整值多项式，则有

$$G^*\{P(h)\}\leqslant 65.$$

5. 如果 $P(h)$ 为 5 次整值多项式，则有

$$G^*\{P(h)\}\leqslant 81.$$

6. 如果 $P(h)$ 为偶的 6 次整值多项式，则有

$$G^*\{P(h)\}\leqslant 2304.$$

7. 如果 $P(h)$ 为 6 次整值多项式，则有

$$G^*\{P(h)\}\leqslant 4627.$$

8. 如果 $P(h)$ 为 7 次整值多项式，则有

$$G^*\{P(h)\}\leqslant 4691.$$

(3) 当 $P(h)$ 为奇的 $k$ 次多项式时，由 Hardy 和 Littlewood[2] 用过的方法，可以证明

$$G\{P(h)\}\leqslant (k-2)2^{k-2}+k+5+\left[\frac{(k-2)\log 2-\log k+\log(k-2)}{\log k-\log(k-1)}\right].$$

虽然对于大的 $k$ 这个上界不是十分好, 但当 $k \leqslant 20$ 时, 它却给出了一些有趣的结果 (见 Hua[3]).

(4) 通过选取特殊的多项式能够改进引理 8.3 中的上界. 可以有许多的选择, 它们使第 7 节中定义的 $\phi(0)=1$, 特别地, 易见

$$G\left\{\frac{1}{2}(x^k+x)\right\} \leqslant 10k^3\log k.$$

## 参考文献


**L.E.Dickson**

[1] On Waring's problem and its generalization. *Annals of Math.*, 1936, 37: 293–316.

**G.H.Hardy and J.E.Littlewood**

[1] Some problems of 'Partitio Numerorum'(IV): The singular series in Waring's problem,and the values of the number $G(k)$. *Math.Zeitschrift*, 1922, 12: 161–188.

[2] Some problems of "Partitio Numerorum"(VI): Further researches in Waring's problem. *Math.Zeitschrift*, 1925, 23: 1–37.

**H.Heilbronn**

[1] Über das Waringsche Problem. *Acta Arith.*, 1935, 1: 212–221.

**L.K.Hua**

[1] On Waring theorems with cubic polynomial summands. *Math.Annalen*, 1935, 111: 622–631.

[2] An easier Waring-Kamke problem. *J.London Math.Soc.*, 1936, 11: 2–3.

[3] On Waring's problem with polynomial summands. *Amer.J.of Math.*, 1936, 58: 553–562.

[4] On Waring's problem with polynomial summands. *J.Chinese Math.Soc.*, 1936, 1: 23–61.

[5] On an exponential sum(印刷中).

**Ralph E.Huston**

[1] Asymptotic generalization of Waring's theorem. *Proc.London Math.Soc.* 1935, 39(2): 82–115.

**R.D.James**

[1] The representation of integers as sums of values of cubic polynomials. *Amer.J.of Math.*, 1934, 56: 303–315.

[2] The representation of integers as sums of pyramidal numbers. *Math.Annalen*, 1934, 109: 189–196.

**E.Kamke**

[1] Verallgemeinerungen des Waring-Hilbertschen Satzes. *Math.Annalen*, 1921, 83: 85–112.

**E.Landau**

[1] Vorlesungen über Zahlentheorie. Bd.1.

[2] Zum Waringschen Problem. *Math.Zeitschrift*, 1938, 12: 219–247.

[3] Über die Winogradoffsche Behandlung des Waringschen Problem. *Math.Zeitschrift*, 1929, 31: 318–338.

[4] Zum Waringschen Problem,Dritte Abhandlung. *Math.Zeitschrift*, 1930, 32: 699–702.

**I.Vinogradov**

[1] On Waring's problem. *Annals of Math.*, 1935, 36: 395–405.

[2] On asymptotic formula in Waring's problem. *Receuil Math.*, 1936, 1(43): 169–174.

[3] A new method of estimation of trigonometric sums. *Receuil Math.*, 1936, 1(43): 175–188.

**E.Maitland Wright**

[1] An extension of Waring's problem. *Phil.Trans.Royal Soc.*, 1933, 232, 1–26.

[2] Proportional conditions in Waring's problem. *Math.Zeitschrift*, 1934, 38: 728–746.

[3] An easier Waring's problem. *J.London Math.Soc.*, 1934, 11: 267–272.

[4] On Tarry's problem I. *Quarterly Journal*, 1935, 6: 261–267.

(贾朝华　译)

# 关于华林问题[①]

华罗庚 (剑桥)

本文的目的是要证明：当 $s \geqslant 2^k+1$ 时，关于丢番图方程

$$N = x_1^k + \cdots + x_s^k \quad (x_\nu \geqslant 0)$$

解数的 Hardy-Littlewood 渐近公式成立. 仅当 $k<14$ 时，这个结果才是新的. 而 $k \geqslant 14$ 时，Vinogradov 的工作要好得多. 最感兴趣的特殊情形是 $k=4$，对此，Estermann[②]，Davenport 和 Heilbronn[③]证明了：每个充分大的整数均为 17 个 4 次幂之和. 但是，他们没有给出解数的渐近公式.

更确切地讲，我所要证明的是下面更一般的

**定理** 设 $P_1(x), \cdots, P_s(x)$ 均为 $k$ 次整值多项式，它们的首项系数分别为正数 $a_1, \cdots, a_s$. 令 $r(N)$ 为丢番图方程

$$N = P_1(x_1) + \cdots + P_s(x_s) \quad (x_\nu \geqslant 0)$$

的解数. 则当 $s \geqslant 2^k+1$ 时，我们有

$$r(N) = \prod_{\nu=1}^{s} a_\nu^{-\frac{1}{k}} \frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)} \mathcal{S}(N) N^{\frac{s}{k}-1} + O(N^{\frac{s}{k}-1-\delta}),$$

这里 $\delta = 2^{1-k}s-2-\varepsilon$，$\varepsilon$ 为任意小的正数，而 $\mathcal{S}(N)$ 如我以前的文章[④]中所定义.

我将另文给出这个定理的一个应用：证明

$$G\{P(x)\} \leqslant 17,$$

其中 $P(x)$ 为 4 次多项式，首项系数为正，且不存在整数 $q(>1)$ 使得

$$P(x) \equiv P(0) (\mathrm{mod} q)$$

---

① 1938 年 2 月 1 日收到. 发表于 *Quarterly Journal of Mathematics, Oxford Series*, 1938, 9: 199–202.

② *Proc. London Math. Soc.*, 1936, 41: 126–142.

③ *Proc. London Math. Soc.*, 1936, 41: 143–150.

④ *Proc. London Math. Soc.*, 1937, 43: 161–182.

恒等地成立.

定理的证明实质上依赖于下面的引理, 而它本身看来也是有趣的.

**主引理**　设 $P(x)$ 是一个 $k$ 次整值多项式,

$$f(\alpha)=\sum_{x=1}^{p}\exp(2\pi \mathrm{i}P(x)\alpha).$$

则有

$$\int_0^1|f(\alpha)|^\lambda \mathrm{d}\alpha=O(p^{\mu(\lambda)}),$$

这里 $(\lambda,\mu(\lambda))$ 位于由顶点 $(2^\nu,2^\nu-\nu+\varepsilon)(\nu=1,\cdots,k)$ 连成的折线上, $O$ 常数仅依赖于 $P(x)$ 的系数和 $\varepsilon$.

关于这个引理在特殊情形 $P(x)=x^k$ 下的改进, 及其在堆垒素数论中的应用, 以后将另文给出.

## 主引理的证明

由于

$$\log\left(\int_0^1|f(\alpha)|^\nu \mathrm{d}\alpha\right)$$

为 $\nu$ 的凸函数①, 我们仅需证明

$$\int_0^1|f(\alpha)|^{2^\nu}\mathrm{d}\alpha=O(p^{2^\nu-\nu+\varepsilon}),\quad \nu=1,2,\cdots,k. \tag{1}$$

不失一般性, 我们可设 $P(x)$ 是一个整系数多项式. 事实上, 令 $q$ 为 $P(x)$ 系数的最小公分母, 由 Hölder 不等式可得

$$\begin{aligned}\int_0^1|f(\alpha)|^\lambda \mathrm{d}\alpha&=\int_0^1\left|\sum_{a=1}^{q}\sum_{x=0}^{[\frac{p-a}{q}]}\exp(2\pi \mathrm{i}P(qx+a)\alpha)\right|^\lambda \mathrm{d}\alpha\\&\leqslant q^{\lambda-1}\sum_{a=1}^{q}\int_0^1\left|\sum_{x=0}^{[\frac{p-a}{q}]}\exp(2\pi \mathrm{i}(P(qx+a)-P(a))\alpha)\right|^\lambda \mathrm{d}\alpha,\end{aligned}$$

这里 $P(qx+a)-P(a)$ 是一个有整系数的多项式.

① 可见 Hardy, Littlewood, Pólya. *Inequalities*, §6.12.

当 $\nu=1$ 时, (1) 式是平凡的; 而当 $\nu=2$ 时, 它是一个熟知的结果①. 我们将用归纳法来证明 (1) 式.

我们将采用缩写

$$\Delta_y Q(x)=\frac{1}{y}(Q(x+y)-Q(x)).$$

假设 $Q(x)$ 是 $h$ 次的多项式, 则 $\Delta_y Q(x)$ 就是 $h-1$ 次的多项式. 用 $\sum_x^p$ 表示变量 $x$ 的项数为 $O(p)$ 的和式.

由于

$$\begin{aligned}|f(\alpha)|^2&=\sum_{x_1=1}^{p}\sum_{x_2=1}^{p}\exp(2\pi\mathrm{i}(P(x_1)-P(x_2))\alpha)\\&=\sum_{x_2}^{p}\sum_{y_1}^{p}\exp(2\pi\mathrm{i}(P(x_2+y_1)-P(x_2))\alpha)\\&=\sum_{y_1}^{p}\sum_{x_2}^{p}\exp(2\pi\mathrm{i}y_1\Delta_{y_1}P(x_2)\alpha),\end{aligned}$$

用 Schwarz 不等式可得

$$\begin{aligned}|f(\alpha)|^4&\ll p\sum_{y_1}^{p}\left|\sum_{x_2}^{p}\exp(2\pi\mathrm{i}y_1\Delta_{y_1}P(x_2)\alpha)\right|^2\\&\ll p\sum_{y_1}^{p}\sum_{y_2}^{p}\sum_{x_3}^{p}\exp(2\pi\mathrm{i}y_1y_2\Delta_{y_2}\Delta_{y_1}P(x_3)\alpha),\end{aligned}$$

这里 $A\ll B$ 意为 $A=O(B)$. 反复这个过程, 对于 $\mu=1,2,\cdots,k-1$ 有

$$\begin{aligned}|f(\alpha)|^{2^\mu}&\ll p^{2^\mu-\mu-1}\sum_{y_1}^{p}\cdots\sum_{y_\mu}^{p}\sum_{x_{\mu+1}}^{p}\exp(2\pi\mathrm{i}y_1\cdots y_\mu\Delta_{y_\mu}\cdots\Delta_{y_1}P(x_{\mu+1})\alpha)\\&\ll p^{2^\mu-1}+p^{2^\mu-\mu-1}\sum_{y_1}^{p}\cdots\sum_{y_\mu}^{p}\sum_{x_{\mu+1}}^{p}{}^{*}\exp(2\pi\mathrm{i}y_1\cdots y_\mu\Delta_{y_\mu}\cdots\Delta_{y_1}P(x_{\mu+1})\alpha),\quad(2)\end{aligned}$$

其中 * 表示条件

$$y_1\cdots y_\mu\Delta_{y_\mu}\cdots\Delta_{y_1}P(x_{\mu+1})\neq 0.$$

因此, 我们可得

$$\int_0^1|f(\alpha)|^{2^\nu}\mathrm{d}\alpha\ll p^{2^{\nu-1}-1}\int_0^1|f(\alpha)|^{2^{\nu-1}}\mathrm{d}\alpha+p^{2^{\nu-1}-\nu}$$

① 可见 Landau, Vorlesungen über Zahlentheorie, Bd.1, 定理 262,37. 他只处理了特殊情形 $P(x)=x^k$. 关于一般情形, 可见华罗庚 (*J.Chinese Math.Soc.*, 1936, 1: 23–61) 的引理 11.

$$\times\int_0^1\sum_{y_1}^{p}\cdots\sum_{y_{\nu-1}}^{p}\sum_{x_\nu}^{p}{}^{*}\exp(2\pi \mathrm{i} y_1\cdots y_{\nu-1}\Delta_{y_{\nu-1}}\cdots\Delta_{y_1}P(x_\nu)\alpha)|f(\alpha)|^{2^{\nu-1}}\mathrm{d}\alpha. \tag{3}$$

由归纳法假设, (3) 式右端的第一项为

$$O(p^{2^{\nu-1}-1}\cdot p^{2^{\nu-1}-\nu+1+\varepsilon})=O(p^{2^\nu-\nu+\varepsilon}).$$

(3) 式右端的第二项为

$$\begin{aligned}&p^{2^{\nu-1}-\nu}\int_0^1\sum_{y_1}^{p}\cdots\sum_{y_{\nu-1}}^{p}\sum_{x_\nu}^{p}{}^{*}\sum_{z_1}^{p}\cdots\sum_{z_{2^\nu-1}}^{p}\exp(2\pi \mathrm{i}(y_1\cdots y_{\nu-1}\Delta_{y_{\nu-1}}\\&\cdots\Delta_{y_1}P(x_\nu)-P(z_1)+P(z_2)-\cdots+P(z_{2^\nu-1}))\alpha)\mathrm{d}\alpha\\=&\ p^{2^{\nu-1}-\nu}R,\end{aligned}$$

这里 $R$ 为方程

$$\begin{cases}y_1\cdots y_{\nu-1}\Delta_{y_{\nu-1}}\cdots\Delta_{y_1}P(x_\nu)=P(z_1)-P(z_2)+\cdots-P(z_{2^\nu-1}),\\ y_1\cdots y_{\nu-1}\Delta_{y_{\nu-1}}\cdots\Delta_{y_1}P(x_\nu)\neq 0, z_\mu, y_\mu, x_\nu\ll P\end{cases} \tag{4}$$

的解数.

对于给定的 $z_1,\cdots,z_{2^\nu-1}$, (4) 式的解数为

$$O(d^{\nu-1}(P(z_1)-P(z_2)+\cdots-P(z_{2^\nu-1})))^{①}.$$

因为 $d(n)=O(n^\varepsilon)$, 所以, 我们有

$$R\ll\sum_{z_1}\cdots\sum_{z_{2^\nu-1}}{}^{\#}\mathrm{d}^{\nu-1}(P(z_1)-P(z_2)+\cdots-P(z_{2^\nu-1}))\ll p^{2^{\nu-1}+\varepsilon},$$

其中 # 表示条件 $P(z_1)-P(z_2)+\cdots-P(z_{2^\nu-1})\neq 0$. 因此, 引理得证.

## 定理的证明

令 $p=N^{\frac{1}{k}}$,

$$S_r(\alpha)=\sum_{x=1}^{p_r}\exp(2\pi \mathrm{i}P_r(x)\alpha),$$

① $d(n)$ 表示 $n$ 的因子个数.

其中 $p_r$ 为 $P_r(x)=N$ 的最大根. 显然, 当 $N$ 充分大时, $p_r$ 总存在且 $p \ll p_r \ll p$. 因而,

$$r(N)=\int_0^1 \prod_{r=1}^{s} S_r(\alpha)\exp(-2\pi i\alpha N)d\alpha.$$

由我以前的文章①中用过的方法, 可知优弧部分容易处理. 所以, 我们只需估计劣弧上的积分 $\overline{W}$.

由 Weyl 定理②和主引理, 我们有

$$\begin{aligned}\overline{W} &\ll p^{(1-2^{1-k}+\varepsilon)(s-2^k)}\int_0^1 \prod_{r=1}^{2^k}|S_r(\alpha)|d\alpha\\ &\ll p^{(1-2^{1-k}+\varepsilon)(s-2^k)}\left(\prod_{r=1}^{2^k}\int_0^1 |S_r(\alpha)|^{2^k}d\alpha\right)^{2^{-k}}\\ &\ll p^{s-k-\delta}.\end{aligned}$$

因此, 定理得证.

在本文结束之际, 我要对审稿人的宝贵意见表示衷心的感谢.

(贾朝华 译)

① *Proc. London Math. Soc.*, 1937, 43: 161–182.

② 见 Landau, *Vorlesungen über Zahlentheorie*, 定理 267.

# 关于 Tarry 问题[①]

华罗庚 (中国, 昆明)

令 $M(k)$ 为最小的正整数 $s$, 使得方程组

$$a_1^h+\cdots+a_s^h=b_1^h+\cdots+b_s^h \quad (1\leqslant h\leqslant k), \tag{1}$$

$$a_1^{k+1}+\cdots+a_s^{k+1}\neq b_1^{k+1}+\cdots+b_s^{k+1} \tag{2}$$

有整数解. 在本文中, 我将证明

$$M(k)\leqslant (k+1)\left(\left[\frac{\log\frac{1}{2}(k+2)}{\log\left(1+\frac{1}{k}\right)}\right]+1\right).$$

所用的方法是非常初等的, 不需要预备知识[②].

本文中, $c_1,c_2,\cdots$ 总表示仅依赖于 $k$ 的正数.

**引理 1** 任意给定一个正数 $H$, 总存在一组正整数 $a_1,\cdots,a_k$(仅依赖于 $k$ 和 $H$), 使得行列式

$$D_k=\begin{vmatrix} 1 & \cdots & 1\\ a_1 & \cdots & a_k\\ \vdots & & \vdots\\ a_1^{k-1} & \cdots & a_k^{k-1}\end{vmatrix}$$

主对角线上的元素之积, 要大于 $D_k$ 的行列式展开式中所有其他项的绝对值之和的 $H$ 倍.

**证明** 我们用归纳法. 设 $\phi_j(a_1,\cdots,a_j)$ 表示 $D_j(j\leqslant k)$ 的主对角线元素之积, 减去 $D_j$ 的行列式展开式中所有其他项的绝对值之和的 $H$ 倍, 则

$$\phi_j(a_1,\cdots,a_j)=a_j^{j-1}\phi_{j-1}(a_1,\cdots,a_{j-1})-H\psi(a_1,\cdots,a_j),$$

---

① 1938 年 5 月 31 日收到. 发表于 *Quarterly Journal of Mathematics, Oxford Series*, 1938, 9: 315–320.

② 由 I.Vinogradov 的一个引理, 我们可以得到 (1) 和 (2) 式在范围 $0\leqslant a_i\leqslant P, 0\leqslant b_i\leqslant P$ 中解数的更清楚的信息. 确切地讲, 我们能够证明这些解的个数 $r(P)$ 满足

$$cP^{2s-\frac{1}{2}k(k+1)}\leqslant r(P)\leqslant c'P^{2s-\frac{1}{2}k(k+1)},$$

其中 $c$ 和 $c'$ 仅依赖于 $k$.

其中 $\psi$ 为 $a_j$ 的 $j-2$ 次多项式. 于是, 如果 $a_1,\cdots,a_{j-1}$ 已经选定使得 $\phi_{j-1}$ 为正, 我们可以再取 $a_j$ 充分大使得 $\phi_j$ 为正. 而最初有 $\phi_1=1$. 因此, 归纳法完成.

**引理 2** 设 $X_1,\cdots,X_k$ 是位于区间

$$a_iQ \leqslant X_i \leqslant 2a_iQ$$

中的整数, 这里 $a_i$ 如引理 1 中所定义. 又设 $N$ 为 $(X_1,\cdots,X_k)$ 的组数, 它们使得

$$X_1^k+\cdots+X_k^k, X_1^{k-1}+\cdots+X_k^{k-1},\cdots,X_1+\cdots+X_k$$

落入给定的长度分别为

$$O(Q^{k-1}),O(Q^{k-2}),\cdots,O(Q),O(1)$$

的区间里面, 则有

$$N=O(1).$$

**证明** 如果 $(X_1,\cdots,X_k)$ 和 $(X_1',\cdots,X_k')$ 为两组满足引理的要求者, 则有

$$X_1^k-X_1'^k+\cdots+X_k^k-X_k'^k=O(Q^{k-1}),$$
$$\cdots\cdots$$
$$X_1-X_1'+\cdots+X_k-X_k'=O(1).$$

令 $Y_i=X_i-X_i'$. 因此, 我们有

$$A_{1,1}Y_1+\cdots+A_{1,k}Y_k=O(Q^{k-1}),$$
$$\cdots\cdots$$
$$A_{k,1}Y_1+\cdots+A_{k,k}Y_k=O(1),$$

其中

$$A_{i,j}=X_j^{k-i}+X_j^{k-i-1}X_j'+\cdots+X_j'^{k-i}.$$

于是,

$$(k-i+1)(a_jQ)^{k-i}\leqslant A_{i,j}\leqslant(k-i+1)(2a_jQ)^{k-i}.$$

考虑行列式 $|A_{i,j}|$. 其主对角线上的元素之积除以 $D_k$ 中的对应项, 要大于

$$k!Q^{k-1+k-2+\cdots+2+1}=k!Q^{\frac{1}{2}k(k-1)}.$$

再者, $|A_{i,j}|$ 的行列式展开式中所有其他项的绝对值之和, 要小于 $D_k$ 中的对应项的

$$2^{\frac{1}{2}k(k-1)}k!Q^{\frac{1}{2}k(k-1)}$$

倍. 由引理 1, 取 $H = 2^{\frac{1}{2}k(k-1)}$, 我们有

$$|A_{i,j}| \geqslant c_1 Q^{\frac{1}{2}k(k-1)}.$$

此外, 又有

$$\begin{vmatrix} O(Q^{k-1}) & A_{1,2} & \cdots & A_{1,k} \\ \vdots & \vdots & & \vdots \\ O(1) & A_{k,2} & \cdots & A_{k,k} \end{vmatrix} = O(Q^{\frac{1}{2}k(k-1)}).$$

因此

$$Y_1 = O(1).$$

类似地

$$Y_2 = O(1), \cdots, Y_k = O(1).$$

这样, 我们就得到了引理.

令 $R_k$ 为方程组

$$\sum_{j=1}^{n}\sum_{i=1}^{k}\chi_{i,j}^h = \sum_{j=1}^{n}\sum_{i=1}^{k}\chi_{i,j}'^h \quad (1 \leqslant h \leqslant k) \tag{3}$$

的解数, 其中 $\chi$ 满足条件

$$a_i P^{(1-\frac{1}{k})^{j-1}} \leqslant \chi_{i,j} \leqslant 2a_i P^{(1-\frac{1}{k})^{j-1}} \quad (i = 1, 2, \cdots, k), \tag{4}$$

而 $\chi'$ 也满足同样的条件. 又令 $R_k'$ 为方程组

$$\sum_{j=1}^{n}\sum_{i=1}^{k}\chi_{i,j}^h = \sum_{j=1}^{n}\sum_{i=1}^{k}\chi_{i,j}'^h \quad (1 \leqslant h \leqslant k-1)$$

的解数, 其中 $\chi$ 和 $\chi'$ 满足与上面同样的条件.

**引理 3**

$$R_k' \geqslant c_2 P^{2k^2(1-(1-\frac{1}{k})^n)-\frac{1}{2}k(k-1)}.$$

**证明** 令 $r(n_1, \cdots, n_{k-1})$ 为方程组

$$\sum_{j=1}^{n}\sum_{i=1}^{k}\chi_{i,j}^h = n_h \quad (1 \leqslant h \leqslant k-1)$$

满足条件 (4) 的解数. 于是, 显然有

$$\sum_{n_1}\cdots\sum_{n_{k-1}} r(n_1, \cdots, n_{k-1}) \geqslant c_3 P^{k(1+(1-\frac{1}{k})+\cdots+(1-\frac{1}{k})^{n-1})} = c_3 P^{k^2(1-(1-\frac{1}{k})^n)},$$

这里和式过所有可能的 $n_1,\cdots,n_{k-1}$. 因为 $c_5P^h\leqslant n_h\leqslant c_6P^h$, 所以, 由 Schwarz 不等式可得

$$\begin{aligned}&\sum_{n_1}\cdots\sum_{n_{k-1}}r(n_1,\cdots,n_{k-1})\\ \leqslant&\sqrt{\sum_{n_1}\cdots\sum_{n_{k-1}}1\cdot\sum_{n_1}\cdots\sum_{n_{k-1}}r^2(n_1,\cdots,n_{k-1})}\\ \leqslant&\sqrt{c_4P^{1+2+\cdots+k-1}\sum_{n_1}\cdots\sum_{n_{k-1}}r^2(n_1,\cdots,n_{k-1})}.\end{aligned}$$

因此

$$\begin{aligned}R_k'=&\sum_{n_1}\cdots\sum_{n_{k-1}}r^2(n_1,\cdots,n_{k-1})\\ \geqslant&c_2P^{2k^2(1-(1-\frac{1}{k})^n)-\frac{1}{2}k(k-1)}.\end{aligned}$$

**引理 4**

$$R_k=O(P^{(2k^2-\frac{1}{2}k(k+1))(1-(1-\frac{1}{k})^n)}).$$

**证明** 由 (3) 和 (4) 式可得

$$\sum_{i=1}^k\chi_{i,1}^h-\sum_{i=1}^k\chi_{i,1}'^h=O(P^{h(1-\frac{1}{k})})\quad(1\leqslant h\leqslant k).$$

于是, 对于固定的 $\chi_{i,1}'(i=1,\cdots,k)$,

$$\sum_{i=1}^k\chi_{i,1}^k,\sum_{i=1}^k\chi_{i,1}^{k-1},\cdots,\sum_{i=1}^k\chi_{i,1}$$

落入长度分别为

$$O(P^{k(1-\frac{1}{k})}),O(P^{(k-1)(1-\frac{1}{k})}),\cdots,O(P^{(1-\frac{1}{k})})\tag{5}$$

的区间里面. 因为区间组 (5) 可以分成

$$\begin{aligned}&O\left(\frac{P^{k(1-\frac{1}{k})}}{P^{k-1}}\cdot\frac{P^{(k-1)(1-\frac{1}{k})}}{P^{k-2}}\cdots\frac{P^{2(1-\frac{1}{k})}}{P}\cdot\frac{P^{1-\frac{1}{k}}}{1}\right)\\ =&O(P^{k-\frac{1}{2}(k+1)})\end{aligned}$$

个长度分别为

$$O(P^{k-1}),O(P^{k-2}),\cdots,O(P),O(1)$$

的区间组, 所以, 由引理 2(取 $Q=P$) 知, $\chi_{i,1}(i=1,\cdots,k)$ 的组数为

$$O(P^{k-\frac{1}{2}(k+1)}).$$

因此, $\chi_{i,1}$ 和 $\chi'_{i,1}(i=1,\cdots,k)$ 的组数为

$$O(P^{2k-\frac{1}{2}(k+1)}).$$

进一步地, 对于固定的 $\chi_{i,j},\chi'_{i,j}(1\leqslant i\leqslant k;1\leqslant j\leqslant l-1)$ 和 $\chi'_{i,l}(1\leqslant i\leqslant k)$, 由 (3) 和 (4) 式, 我们可见

$$\sum_{i=1}^{k}\chi_{i,l}^{k},\sum_{i=1}^{k}\chi_{i,l}^{k-1},\cdots,\sum_{i=1}^{k}\chi_{i,l}$$

落入长度分别为

$$O(P^{k(1-\frac{1}{k})^{l}}),O(P^{(k-1)(1-\frac{1}{k})^{l}}),\cdots,O(P^{(1-\frac{1}{k})^{l}}) \tag{6}$$

的区间里面. 因为

$$\begin{aligned}&O\left(\frac{P^{k(1-\frac{1}{k})^{l}}}{P^{(k-1)(1-\frac{1}{k})^{l-1}}}\cdot\frac{P^{(k-1)(1-\frac{1}{k})^{l}}}{P^{(k-2)(1-\frac{1}{k})^{l-1}}}\cdots\frac{P^{(1-\frac{1}{k})^{l}}}{1}\right)\\&=O(P^{(k-\frac{1}{2}(k+1))(1-\frac{1}{k})^{l-1}}),\end{aligned}$$

所以, 由引理 2(取 $Q=P^{(1-\frac{1}{k})^{l-1}}$) 知, $\chi_{i,l}(1\leqslant i\leqslant k)$ 的组数为

$$O(P^{(k-\frac{1}{2}(k+1))(1-\frac{1}{k})^{l-1}}).$$

因此, 对于固定的 $\chi_{i,j},\chi'_{i,j}(1\leqslant i\leqslant k;1\leqslant j\leqslant l-1),\chi_{i,l}$ 和 $\chi'_{i,l}$ 的组数为

$$O(P^{(2k-\frac{1}{2}(k+1))(1-\frac{1}{k})^{l-1}}).$$

合之可得, 在限制条件 (4) 之下, (3) 式的总解数为

$$\begin{aligned}&O(P^{(2k-\frac{1}{2}(k+1))(1+(1-\frac{1}{k})+\cdots+(1-\frac{1}{k})^{n-1})})\\&=O(P^{(2k^{2}-\frac{1}{2}k(k+1))(1-(1-\frac{1}{k})^{n})}).\end{aligned}$$

**定理**　如果 $n>\log\frac{1}{2}(k+1)/(\log k-\log(k-1))$, 则存在无穷多组整数满足

$$\sum_{j=1}^{n}\sum_{i=1}^{k}\chi_{i,j}^{h}=\sum_{j=1}^{n}\sum_{i=1}^{k}\chi_{i,j}^{\prime h}\quad(1\leqslant h\leqslant k-1),$$

$$\sum_{j=1}^{n}\sum_{i=1}^{k}\chi_{i,j}^{k}\neq\sum_{j=1}^{n}\sum_{i=1}^{k}\chi_{i,j}^{\prime k}.$$

**证明** 我们考虑那些满足 (4) 式的 $\chi_{i,j}$ 和 $\chi'_{i,j}$. 显然, 定理中方程组的解数就等于

$$R'_k - R_k.$$

对于充分大的 $P$, 因为

$$n > \frac{\log\frac{1}{2}(k+1)}{\log k - \log(k-1)},$$

所以, 由引理 3 和 4 知,

$$\begin{aligned} R'_k - R_k &\geqslant c_2 P^{2k^2(1-(1-\frac{1}{k})^n)-\frac{1}{2}k(k-1)} \\ &\quad - O(P^{(2k^2-\frac{1}{2}k(k+1))(1-(1-\frac{1}{k})^n)}) \\ &\geqslant c_7 P^{2k^2(1-(1-\frac{1}{k})^n)-\frac{1}{2}k(k-1)}. \end{aligned}$$

由此立得定理.

在定理中用 $k+1$ 代替 $k$, 我们可得

$$M(k) \leqslant (k+1)\left(\left[\frac{\log\frac{1}{2}(k+2)}{\log\left(1+\frac{1}{k}\right)}\right]+1\right).$$

由此可以推出

$$\overline{\lim_{k\to\infty}} \frac{M(k)}{k^2\log k} \leqslant 1.$$

下面我将指出如何改进右端的常数. 但是, 我们无法改进它的阶.

设 $k = 2l-1$ 是一个奇数. 令 $J(l)$ 为最小的正整数 $s$, 使得

$$\sum_{i=1}^{s} \chi_i^{2h} = \sum_{i=1}^{s} \chi_i'^{2h} \quad (h = 1, \cdots, l-1),$$

$$\sum_{i=1}^{s} \chi_i^{2l} \neq \sum_{i=1}^{s} \chi_i'^{2l}$$

可解. 用上面的方法, 我们可以证明

$$J(l) \leqslant l\left[\frac{\log\frac{1}{2}(l+1)}{\log l - \log(l-1)}+1\right].$$

明显地, 如果

$$\begin{aligned} &a_1^{2h} + \cdots + a_s^{2h} = b_1^{2h} + \cdots + b_s^{2h} \quad (1 \leqslant h \leqslant l-1), \\ &a_1^{2l} + \cdots + a_s^{2l} \neq b_1^{2l} + \cdots + b_s^{2l}, \end{aligned}$$

则有

$$\begin{aligned}&\sum_{i=1}^{s}((x+a_i)^t+(x-a_i)^t)\\=&\sum_{i=1}^{s}((x+b_i)^t+(x-b_i)^t)\quad(1\leqslant t\leqslant 2l-1),\end{aligned}$$

$$\sum_{i=1}^{s}((x+a_i)^{2l}+(x-a_i)^{2l})\neq\sum_{i=1}^{s}((x+b_i)^{2l}+(x-b_i)^{2l}).$$

于是, 我们有

$$\begin{aligned}M(k)\leqslant 2J(l)\leqslant 2l&\left[\frac{\log\frac{1}{2}(l+1)}{\log l-\log(l-1)}+1\right]\\&\leqslant(k+1)\left[\frac{\log\frac{1}{4}(k+3)}{\log(k+1)-\log(k-1)}+1\right]\\&\sim\frac{1}{2}k^2\log k.\end{aligned}$$

另一种方法是重新考虑 (3) 式中的 "尾巴", 即对应于 $\chi_{i,n}$ 和 $\chi'_{i,n}$ 的部分. 用此方法可以在结果中减去一个 $>\frac{1}{2}k$ 的数.

注 1. 当 $k\geqslant 15$ 时, 这里给出的结果要好于 E.M.Wright 的结果. 他证明了, 当 $k\geqslant 12$ 时, 有

$$M(k)<\frac{7k^2(k-11)(k+3)}{216}.$$

注 2. 当我们将 $a$ 和 $b$ 限制为素数时, 定理仍然适用.

(贾朝华　译)

# 表整数为素数幂之和[①] [②]

华罗庚[③](剑桥)

设 $k(\geqslant 4)$ 是一个整数, $a=\dfrac{1}{k}$,

$$b=\begin{cases} k^3(\log k+1.25\log\log k^2), & \text{当 } k\geqslant 15 \text{ 时},\\ 2^{k-1}, & \text{当 } k<15 \text{ 时},\end{cases}$$

而

$$m=\left[\frac{\log\frac{b}{2}+\log(1-2a)}{\log k-\log(k-1)}\right].$$

设 $p^\theta \parallel k$,

$$\gamma=\begin{cases} \theta+2, & \text{当 } p=2, 2|k \text{ 时},\\ \theta+1, & \text{其他},\end{cases}$$

$$K=\prod_{(p-1)|k} p^\gamma.$$

**定理** 当 $s\geqslant s_0$ 时, 每个充分大的整数 $N\equiv s(\bmod K)$ 可表为 $s$ 个素数的 $k$ 次幂之和, 这里 $s_0=s_0(k)=2k+2m+7$.

值得注意的是: 对于大的 $k, s_0$ 的阶为 $6k\log k$, 这和 Vinogradov 关于华林问题的结果[④]一样好; 而对于小的 $k$, 有 $s_0(4)=19, s_0(5)=31$, 这很接近于 Davenport, Estermann 和 Heilbronn 的结果[⑤]. 本文的方法也可用来证明: 当 $s\geqslant k+m+4(\sim 3k\log k)$ 时, 几乎所有的整数 $N\equiv s(\bmod K)$ 都可表为 $s$ 个素数的 $k$ 次幂之和.

对于 $k=3$, 本文的方法给出[⑥] $s_0(3)=11$.

---

① 1938 年 2 月 28 日收到. 发表于 *Mathematische Zeitschrift*,1939, 44(3): 335–346.

② 关于结果的一些初步描述已经发表在*Comptes Rendus de l'USSR*,1937, 17(5).

③ 时任中华教育与文化促进基金会研究员.

④ On the upper bound of $G(n)$ in Waring's problem. *Bull. de l'Acad. de l'URSS, VII Serie*, Classe des sciences math. naturelles, 1934: 1455–1469; Une nouvelle variante de la demonstration du theorem de Waring. *Compte Rendus*, 1935, 200: 182–184; On Waring's problem.*Annals of Math.*, 1935, 36: 395–405.

⑤ *Proc. of London Math. Soc.*, 1936, 41(2): 26–150.

⑥ 作者已经找到了一种新方法, 由它可以证明: 每个充分大的奇数可以表为 9 个素数的立方之和. 这将另文发表.

本文由三部分组成：

1. 奇异级数的研究.
2. 关于华林问题的一个引理.
3. 定理的证明.

## 1. 奇异级数的研究

设

$$W_{h,q}=\sum_{\substack{l=1\\(l,q)=1}}^{q} e_q(hl^k),\quad e_q(x)=\mathrm{e}^{\frac{2\pi ix}{q}},$$

$$B_s(N,q)=\sum_{\substack{h=1\\(h,q)=1}}^{q}\left(\frac{W_{h,q}}{\varphi(q)}\right)^s e_q(-hN),$$

$$S(N)=\sum_{q=1}^{\infty}B_s(N,q).$$

**引理 1.1** 如果 $(q_1,q_2)=1$, 则有

$$W_{h,q_1q_2}=W_{hq_1^{k-1},q_2}W_{hq_2^{k-1},q_1}$$

以及

$$B_s(N,q_1q_2)=B_s(N,q_1)B_s(N,q_2).$$

**证明** 令 $l=l_1q_2+l_2q_1$, 则

$$\begin{aligned}W_{h,q_1q_2}&=\sum_{\substack{l_1=1\\(l_1,q_1)=1}}^{q_1}\sum_{\substack{l_2=1\\(l_2,q_2)=1}}^{q_2} e_{q_1q_2}(hq_2^kl_1^k+hq_1^kl_2^k)\\&=W_{hq_1^{k-1},q_2}W_{hq_2^{k-1},q_1}.\end{aligned}$$

第二个结论是前一个的直接推论.

**引理 1.2** 如果 $t>\gamma$, 则有

$$W_{h,p^t}=0.$$

**证明** 令 $l=l_1+l_2p^{t-\theta-1}$. 由 Landau①的定理 290(对 $p=2$ 作一点简单的修改), 我们有

$$W_{h,p^t}=\sum_{\substack{l_1=1\\(l_1,p)=1}}^{p^{t-\theta-1}}\sum_{l_2=1}^{p^{\theta+1}} e_{p^t}(h(l_1^k+p^{t-\theta-1}kl_1^{k-1}l_2))=0,$$

① *Vorlesungen über Zahlentheorie, Bd.1.* 这个注释在相似的场合就不再重复了.

这里用到了 $p \nmid l_1 k p^{-\theta}$.

**引理 1.3**

$$W_{h,q} = O(q^{\frac{1}{2}+\varepsilon}),$$

这里 $O$ 常数依赖于 $k$ 和 $\varepsilon$.

**证明** 由引理 1.2 知,

$$\begin{aligned} &W_{h,p^t} = O(1), \quad \text{当 } p|k \text{ 时}, \\ &W_{h,p^t} = 0, \quad \text{当 } p \nmid k \text{ 且 } t > 1 \text{ 时}. \end{aligned}$$

进一步地, 由 Landau 的定理 311, 我们有

$$|W_{h,p}| \leqslant \begin{cases} k\sqrt{p}, & \text{对于所有的 } p, \\ p^{\frac{1}{2}+\varepsilon}, & \text{对于 } p \geqslant k^{\frac{1}{\varepsilon}}. \end{cases}$$

设 $q = p_1^{t_1} \cdots p_v^{t_v}$ 且 $p_1 < p_2 < \cdots < p_v$. 则由引理 1.1 可得

$$|W_{h,q}| = \prod_{p_i \leqslant k^{\frac{1}{\varepsilon}}} |W_{h_i, p_i^{t_i}}| \prod_{p_i > k^{\frac{1}{\varepsilon}}} |W_{h_i, p_i^{t_i}}| = O(q^{\frac{1}{2}+\varepsilon}).$$

**引理 1.4** 如果 $s > 4$, 则

$$\mathcal{S}(N) = \prod_p \chi_p(N),$$

其中

$$\chi_p(N) = 1 + \sum_{t=1}^{\gamma} B_s(N, p^t).$$

**证明** 由引理 1.1,1.2 和 1.3 可得.

**引理 1.5** 令 $M_s(p^t, N)$ 为同余式

$$x_1^k + \cdots + x_s^k \equiv N(\text{mod} p^t), \quad p \nmid x_1 \cdots x_s, \quad 0 < x_i < p^t$$

的解数. 则有

$$\varphi(p^t)^{-s} p^t M_s(p^t, N) = 1 + \sum_{d=1}^{t} B_s(N, p^d).$$

**证明** 我们有

$$M_s(p^t, N) = p^{-t} \sum_{\substack{l_1=1 \\ (l_1,p)=1}}^{p^t} \cdots \sum_{\substack{l_s=1 \\ (l_s,p)=1}}^{p^t} \sum_{h=1}^{p^t} e_{p^t}(h(l_1^k + \cdots + l_s^k - N))$$

$$= p^{-t}\sum_{h=1}^{p^t} W_{h,p^t}^s e_{p^t}(-hN)$$

$$= p^{-t}\varphi^s(p^t)\left(1+\sum_{d=1}^{t} B_s(N,p^d)\right).$$

**引理 1.6** (I.Chowla 和 Davenport)① 设 $x_1,\cdots,x_m$ 属于 $m$ 个不同的剩余类 mod$p^l$, 而 $y_1,\cdots,y_n$ 属于 $n$ 个不同的剩余类 mod$p^l$, 且任两个 $y_j$ 互不同余 mod$p$. 则由

$$x_i+y_j \quad (1\leqslant i\leqslant m, 1\leqslant j\leqslant n)$$

所表示的不同剩余类的个数大于或等于

$$\min(m+n-1,p^l).$$

**引理 1.7** 当 $s\geqslant 4k$ 且 $(p-1)\nmid k$ 时, 有

$$M_s(p^\gamma,N)>0.$$

**证明** 1) $p\nmid k$. 此时, 有 $\gamma=1$. 因为 $(p-1)\nmid k$, 所以, 当 $x$ 跑过 $1,2,\cdots,p-1(\bmod p)$ 时, $x^k$ 给出

$$d=\frac{p-1}{k,p-1}>0$$

个不同值 mod$p$. 因为

$$s\geqslant 4k\geqslant \frac{p^\gamma-1}{\frac{d}{2}}\geqslant\frac{p^\gamma-1}{d-1},$$

所以, 由引理 1.6, $x_1^k+\cdots+x_s^k(p\nmid x_1\cdots x_s)$ 给出

$$\min(d+(d-1)(s-1),p)=p$$

个不同值 mod$p$.

2) $k=p^\theta k_0, p\nmid k_0$. 因为

$$x^{p^\theta k_0}\equiv x^{k_0}(\bmod p) \text{ 和 } (k_0,p-1)=1,$$

所以, $x^k$ 给出至少 $p-1$ 个两两互不同余 mod$p$ 的值. 又因为

$$s\geqslant 4k\geqslant 4p^\theta\geqslant\frac{p^\gamma-p+1}{p-2}+1,$$

① 可见 Landau. Über einige neuere Fortschritte der additiven Zahlentheorie. *Cambridge Tracts*,no.35, 第 8 页.

所以, $x_1^k+\cdots+x_s^k$ 给出

$$\min(p-1+(p-2)(s-1),p^{\gamma})=p^{\gamma}$$

个不同值 $\bmod p^{\gamma}$.

**引理 1.8** 如果 $s\equiv N(\bmod p^{\gamma})$ 且 $(p-1)|k$, 则有

$$M_s(p^{\gamma},N)>0.$$

显然.

**引理 1.9** 如果 $s\geqslant 4k$, 且对于所有满足 $(p-1)|k$ 的 $p$, 有 $s\equiv N(\bmod p^{\gamma})$, 则

$$\mathcal{S}(N)\geqslant A(与N无关)>0.$$

**证明** 用引理 1.5,1.7 和 1.8, 对于所有的 $p$, 我们可得

$$\chi_p>0.$$

由 Landau 的定理 311 知

$$|B_s(N,p)|\leqslant\frac{(k\sqrt{p})^s}{(p-1)^{s-1}}\leqslant(2k)^s p^{-\frac{s}{2}+1}.$$

因而, 对于 $p>(2k)^{4s}$, 有

$$\chi_p>1-p^{-\frac{s}{2}+1+\frac{1}{4}}.$$

我们可得

$$\mathcal{S}(N)\geqslant\prod_{p\leqslant(2k)^{4s}}\chi_p\prod_{p>(2k)^{4s}}(1-p^{-\frac{5}{4}})\geqslant A>0.$$

**注**: 同理, 我们可以证明: 当 $k=3$ 而 $s=11$ 或 9 时, 对于所有的奇数 $N$ 有

$$\mathcal{S}(N)\geqslant A>0.$$

## 2. 关于华林问题的一个引理

设 $N$ 是一个大的整数, $P=\frac{1}{2}N^a$,

$$T(\alpha,P)=\sum_{P<n<2P}e(n^k\alpha),\quad e(x)=\mathrm{e}^{2\pi\mathrm{i}x},$$

$$T_i(\alpha)=T(\alpha,\alpha^{-i}P^{(1-a)^i})\quad(i=0,\cdots,m+1),$$

$$Q(\alpha)=T_1(\alpha)\cdots T_m(\alpha)T_{m+1}^2(\alpha)=\sum_n r_{m+2}(n)e(n\alpha),$$

$$R(\alpha)=T_0(\alpha)Q(\alpha)=\sum_n r_{m+3}(n)e(n\alpha),$$

$$T_0^k(\alpha)R(\alpha)=\sum_n r_{k+m+3}(n)e(n\alpha).$$

令 $c_1,c_2,\cdots$ 为仅依赖于 $k$ 的数. 于是,

$$c_1P^{k-1-(k-2)(1-a)^{m+1}}\leqslant Q(0)\leqslant c_2P^{k-1-(k-2)(1-a)^{m+1}}.$$

下面的 $O$ 常数仅依赖于 $k$ 和 $\varepsilon$, 其中 $\varepsilon$ 为任意小的正数.

本节的目的是要证明

$$\sum_n r_{k+m+3}^2(n)=O(P^{k+2}Q^2(0)).$$

我们按通常的方式, 将区间 $0\leqslant\alpha\leqslant1$ 分成属于所有有理点 $\frac{h}{q}(1\leqslant q\leqslant P^{k-1+\epsilon},0<h<q,(h,q)=1)$ 的 Farey 弧. 每个弧都有形式

$$\alpha=\frac{h}{q}+\beta,\quad -\frac{\theta_1}{qP^{k-1+\varepsilon}}\leqslant\beta\leqslant\frac{\theta_2}{qP^{k-1+\varepsilon}},$$

其中 $\frac{1}{2}\leqslant\theta_i\leqslant1$.

令 $M_{h,q}$ 表示一个弧 (或弧的一部分), 它满足

$$q\leqslant P^{\frac{k}{b}},\quad |\beta|\leqslant\frac{1}{qP^{k(1-\frac{1}{b})}}.$$

而令 $E$ 为不属于任何 $M_{h,q}$ 的点集.

设

$$S_{h,q}=\sum_{v=1}^{q}e_q(v^kh),$$

以及

$$T^*(\alpha,h,q)=q^{-1}S_{h,q}\int_P^{2P}\mathrm{e}^{2\pi iy^k\beta}\mathrm{d}y.$$

**引理 2.1**① 如果 $(h,q)=1$, 则

$$S_{h,q}=O(q^{1-a}).$$

① Landau 的定理 315.

**引理 2.2** (Davenport 和 Heilbronn)①

$$\sum_{x=1}^{m} e_q(hx^k) = \frac{m}{q} S_{h,q} + O(q^{\frac{3}{4}+\varepsilon}).$$

因此, 如果 $m \leqslant q$, 则对于 $k \geqslant 4$, 有

$$\sum_{x=1}^{m} e_q(hx^k) = O(q^{1-a+\varepsilon}).$$

**引理 2.3** (Wey②和 Vinogradov③) 如果 $\alpha$ 属于对应 $P^{1-\varepsilon} < q \leqslant P^{k-1+\varepsilon}$ 的弧, 则有

$$T(\alpha) = O(P^{1-\frac{1}{b}+\varepsilon}).$$

**引理 2.4**

$$\int_0^1 |R(\alpha)|^2 \mathrm{d}\alpha = \sum_n r_{m+3}^2(n) = O(P^{1+\varepsilon} Q(0)).$$

**证明** $\sum_n r_{m+3}^2(n)$ 为方程

$$x_0^k + \cdots + x_m^k + x_{m+1}^k + x_{m+1}'^k = y_0^k + \cdots + y_m^k + y_{m+1}^k + y_{m+1}'^k,$$
$$2^{-i} P^{(1-a)^i} \leqslant x_i, y_i \leqslant 2^{1-i} P^{(1-a)^i}$$

的解数. 当 $P$ 充分大时, 总有 $x_i = y_i (i = 0, 1, \cdots, m)$. 如若不然, 设 $v$ 为第一个使 $x_v \neq y_v$ 的下标, 于是, 当 $P$ 充分大时,

$$|x_v^k - y_v^k| \geqslant k(P^{(1-a)^v} 2^{-v})^{k-1}$$

必定大于

$$y_{v+1}^k + \cdots + y_{m+1}'^k,$$

可得出矛盾. 由熟知的结果, 方程

$$x_{m+1}^k + x_{m+1}'^k = y_{m+1}^k + y_{m+1}'^k$$

的解数为 $O(P^{2(1-a)^{m+1}+\varepsilon})$. 引理得证.

**引理 2.5**

$$T^*(\alpha, h, q) = O(q^{-a} \min(P, |\beta|^{-a})).$$

① *Proc.of London Math.Soc.*, 1936, 41(2): 449–453.
② Landau 的定理 267.
③ 我要感谢 Vinogradov 教授告诉我这个新结果.

**证明** 因为

$$S_{h,q}=O(q^{1-a}),$$

以及

$$\int_P^{2P} e^{2\pi i\beta y^k}dy=O(P),$$

所以, 只需证明

$$\int_P^{2P} e^{2\pi i\beta y^k}dy=O(|\beta|^{-a})$$

即可. 而这由变量替换立得.

**引理 2.6** 如果 $q\leqslant P^{1-\varepsilon},|\beta|\leqslant q^{-1}P^{-k+1-\varepsilon}$, 则有

$$T(\alpha)-T^*(\alpha,h,q)=O(q^{1-a+\varepsilon}).$$

**证明** 由 Estermann 的讨论 (§§2.4–2.7)①, 并用引理 2.2 代替 Weyl 的估计, 可以证明引理.

**引理 2.7**

$$\int_E |T_0^k(\alpha)R(\alpha)|^2 d\alpha=O(P^{k+2-c_3}Q^2(0)).$$

**证明** 因为 $\alpha$ 不在 $M_{h,q}$ 中, 所以, 下面三个条件至少有一个满足:

(i) $P^{1-\varepsilon}<q\leqslant P^{k-1+\varepsilon}$;

(ii) $P^{\frac{k}{b}}<q\leqslant P^{1-\varepsilon}$;

(iii) $q\leqslant P^{\frac{k}{b}},|\beta|>q^{-1}P^{-k(1-\frac{1}{b})}$.

由引理 2.3,2.5 和 2.6, 在 $E$ 上, 我们有

$$T_0(\alpha)=O(P^{1-\frac{1}{b}}).$$

再由引理 2.4, 可得

$$\begin{aligned}&\int_E |T_0^{2k}(\alpha)R^2(\alpha)|d\alpha\\&=O(P^{2k(1-\frac{1}{b})}\int_0^1 |R(\alpha)|^2 d\alpha)\\&=O(P^{2k(1-\frac{1}{b})+1+\varepsilon}Q(0))\\&=O(P^{2k(1-\frac{1}{b})+2-k+(k-2)(1-a)^{m+1}}Q^2(0))\\&=O(P^{k+2-c_3}Q^2(0)),\end{aligned}$$

这里用到了

① *Proc. of London Math. Soc.*, 1936, 41(2): 126–143.

$$\begin{aligned}&-\frac{2k}{b}+(k-2)(1-a)^{m+1}\\<&-\frac{2k}{b}+(k-2)(1-a)^{\log\frac{b}{2}(1-2a)/\log(1-a)^{-1}}\\=&-\frac{2k}{b}+(k-2)\left(\frac{b}{2}(1-2a)\right)^{-1}=0.\end{aligned}$$

**引理 2.8**

$$\sum_{M}\int_{M}|T_0^k(\alpha)R(\alpha)|^2\mathrm{d}\alpha=O(P^{k+2}Q^2(0)).$$

**证明** 由引理 2.5 和 2.6, 在 $M$ 上, 我们有

$$\begin{aligned}T_0(\alpha)&=O(q^{-a}\min(P,|\beta|^{-a}))+O(q^{1-a+\varepsilon})\\&=O(q^{-a}\min(P,|\beta|^{-a})).\end{aligned}$$

所要估计的和式不超过

$$\begin{aligned}&O\left(\sum_{M}\int_{M}q^{-2(k+1)a}\min(P^{2(k+1)},|\beta|^{-2(1+a)})Q^2(0)\mathrm{d}\beta\right)\\=&O\left(\sum_{q}q^{-1-2a}P^{k+2}Q^2(0)\right)\\=&O(P^{k+2}Q^2(0)).\end{aligned}$$

**引理 2.9**

$$\sum_{n}r_{k+m+3}^2(n)=O(P^{k+2}Q^2(0)).$$

**证明** 由引理 2.7 和 2.8, 可得本引理.

## 3. 定理的证明

令

$$\Im(\alpha,P)=\sum_{P<p<2P}e(p^k\alpha).$$

相应地, 我们定义 $\Im_i(\alpha)(i=0,1,\cdots,m,m+1)$, $\mathfrak{H}(\alpha)$ 和 $\Re(\alpha)$. 再令

$$\Im_0^{k+1}(\alpha)\mathfrak{H}(\alpha)=\sum_{n}r'_{m+k+3}(n)e(n\alpha)$$

和

$$\Im_0^{2k+3}(\alpha)\mathfrak{H}^2(\alpha)=\sum_{n}r'_{2m+2k+7}(n)e(n\alpha),$$

因此, $r'_{2m+2k+7}(n)$ 为方程

$$n = p_1^k + \cdots + p_{2m+2k+7}^k$$

的解数, 其中 $p_i$ 满足一定的条件.

令

$$\Im_0^*(\alpha, h, q) = \frac{W_{h,q}}{\varphi(q)} \sum_{P^k \leqslant n \leqslant (2P)^k} \frac{e(n\beta)}{n^{1-a}\log n}.$$

我们将区间 $0 \leqslant \alpha \leqslant 1$分成属于所有有理点 $\frac{h}{q}(1 \leqslant q \leqslant NL^{-\sigma_0}, 0 \leqslant h \leqslant q, (h,q) = 1)$ 的 Farey 弧, 其中 $L = \log N, \sigma_0$ 是使引理 3.1 成立的数. 我们再将这些弧分成优弧 $M(1 \leqslant q \leqslant L^{\sigma_0})$ 和劣弧 $m(L^{\sigma_0} \leqslant q \leqslant NL^{-\sigma_0})$. 在两种情形中, 弧均有形式

$$\alpha = \frac{h}{q} + \beta, \quad -\frac{\theta_1 L^{\sigma_0}}{qN} \leqslant \beta \leqslant \frac{\theta_2 L^{\sigma_0}}{qN},$$

其中 $\frac{1}{2} \leqslant \theta_i \leqslant 1$.

**引理 3.1** (Vinogradov)[①]　存在一个整数 $\sigma_0$, 使得在 $m$ 上, 有

$$\Im_0(\alpha) = O(PL^{-\sigma}).$$

特别地, 我们可以取 $\sigma_0$ 使得 $\sigma \geqslant 2k + 2m + 8$.

**引理 3.2**

$$\sum_m \int_m |\Im_0^{2k+3}(\alpha)\mathfrak{H}^2(\alpha)| \mathrm{d}\alpha = O(P^{k+3}Q^2(0)L^{-\sigma}).$$

**证明**　由引理 2.9 和 3.1, 我们有

$$\begin{aligned}
&\sum_m \int_m |\Im_0^{2k+3}(\alpha)\mathfrak{H}^2(\alpha)| \mathrm{d}\alpha \\
=&O\left(PL^{-\sigma} \int_0^1 |\Im_0^{k+1}(\alpha)\mathfrak{H}(\alpha)|^2 \mathrm{d}\alpha\right) \\
=&O\left(PL^{-\sigma} \sum_n r'^2_{m+k+3}(n)\right) \\
=&O\left(PL^{-\sigma} \sum_n r^2_{m+k+3}(n)\right) \\
=&O\left(P^{k+2}Q^2(0)PL^{-\sigma}\right).
\end{aligned}$$

① *Comptes Rendus de l'URSS*, 1937, 16(3).

**引理 3.3** (Siegel-Walfisz)① 如果 $q \leqslant L^{\sigma_0}, (l,q)=1, n \leqslant N$, 则

$$\pi(n;l,q)=\frac{1}{\varphi(q)}\mathrm{li}n+O(N\mathrm{e}^{-c_4\sqrt{L}}).$$

**引理 3.4** 在 $M$ 上, 有

$$\Im_0(\alpha)-\Im_0^*(\alpha,h,q)=O(P\mathrm{e}^{-c_5\sqrt{L}}).$$

这是引理 3.3 的一个推论②.

**引理 3.5**

$$\Im_0^*(\alpha,h,q)=O(q^{-\frac{1}{2}+\varepsilon}\min(P,|\beta|^{-a})).$$

这是引理 1.2 的推论.

**引理 3.6**

$$\sum_M\int_M|\Im_0^{2k+3}(\alpha)-\Im_0^{*2k+3}(\alpha,h,q)||\mathfrak{H}^2(\alpha)|\mathrm{d}\alpha$$
$$=O(P^{k+3}Q^2(0)\mathrm{e}^{-c_6\sqrt{L}}).$$

**证明** 由引理 3.4 和 3.5, 在 $M$ 上, 有

$$\begin{aligned}\Im_0^{2k+3}(\alpha)-\Im_0^{*2k+3}(\alpha,h,q)&=O((PL^{-\frac{1}{2}\sigma_0})^{2k+2}P\mathrm{e}^{-c_5\sqrt{L}})\\&=O(P^{2k+3}\mathrm{e}^{-c_7\sqrt{L}}).\end{aligned}$$

因此, 所要估计的和式不超过

$$O\left(\sum_{q\leqslant L^{\sigma_0}}q\cdot P^{2k+3}\mathrm{e}^{-c_7\sqrt{L}}\cdot q^{-1}N^{-1}L^{\sigma_0}Q^2(0)\right)$$
$$=O(P^{k+3}Q^2(0)\mathrm{e}^{-c_6\sqrt{L}}).$$

**引理 3.7**

$$\sum_M\int_M|\Im_0^{*2k+3}(\alpha,h,q)|\left|\mathfrak{H}^2(\alpha)-\Lambda^2\left(\frac{W_{h,q}}{\varphi(q)}\right)^{2m+4}\right|\mathrm{d}\alpha$$
$$=O(P^{k+3}Q^2(0)\mathrm{e}^{-c_8\sqrt{L}}),$$

这里

$$c_9\frac{Q(0)}{L^{m+2}}\leqslant\Lambda\leqslant c_{10}\frac{Q(0)}{L^{m+2}}.$$

① *Math.Zeitschr.*, 1936, 40: 592–601.

② 可见 Davenport 和 Heilbronn. *Proc.of London Math.Soc.*, 1931, 43(2): 142–151, 引理 2.

**证明** 我们有

$$\begin{aligned}\left|\mathfrak{H}(\alpha)-\mathfrak{H}\left(\frac{h}{q}\right)\right| &\leqslant \sum_n r'_{m+2}(n)\left|e(n\alpha)-e\left(n\frac{h}{q}\right)\right|\\ &\leqslant |\beta|\sum_n nr'_{m+2}(n)\\ &=O(P^{k-1}|\beta|Q(0))\\ &=O(P^{-1}L^{\sigma_0}Q(0)).\end{aligned}$$

进一步地, 由引理 3.3 知

$$\begin{aligned}\mathfrak{I}_i\left(\frac{h}{q}\right) &= \sum_{2^{-i}P^{(1-a)^i}<p\leqslant 2^{-i+1}P^{(1-a)^i}} e_q(hp^k)\\ &= \sum_{\substack{l=1\\(l,q)=1}}^{q} e_q(hl^k)(\pi(2^{-i}P^{(1-a)^i};l,q)-\pi(2^{-i+1}P^{(1-a)^i};l,q))+O(q^{\varepsilon})\\ &= \frac{W_{h,q}}{\varphi(q)}\int_{2^{-i}P^{(1-a)^i}}^{2^{-i+1}P^{(1-a)^i}}\frac{\mathrm{d}x}{\log x}+O(P^{(1-a)^i}\mathrm{e}^{-c_{11}\sqrt{L}}).\end{aligned}$$

从而有

$$\mathfrak{H}\left(\frac{h}{q}\right)=\left(\frac{W_{h,q}}{\varphi(q)}\right)^{m+2}\Lambda+O(Q(0)\mathrm{e}^{-c_{12}\sqrt{L}}),$$

其中

$$\Lambda=\left(\prod_{i=1}^{m+1}\int_{2^{-i}P^{(1-a)^i}}^{2^{-i+1}P^{(1-a)^i}}\frac{\mathrm{d}x}{\log x}\right)\left(\int_{2^{-(m+1)}P^{(1-a)^{m+1}}}^{2^{-m}P^{(1-a)^{m+1}}}\frac{\mathrm{d}x}{\log x}\right).$$

显然, $\Lambda$ 满足引理中的不等式.

因此

$$\begin{aligned}\left|\mathfrak{H}^2(\alpha)-\Lambda^2\left(\frac{W_{h,q}}{\varphi(q)}\right)^{2(m+2)}\right| &\leqslant \left|\mathfrak{H}(\alpha)-\Lambda\left(\frac{W_{h,q}}{\varphi(q)}\right)^{m+2}\right|Q(0)\\ &=O(Q^2(0)\mathrm{e}^{-c_{12}\sqrt{L}}).\end{aligned}$$

由引理 3.5, 所要估计的和式不超过

$$O\left(\sum_{q\leqslant L^{\sigma_0}}q\cdot Q^2(0)\mathrm{e}^{-c_{12}\sqrt{L}}q^{-\frac{2k+3}{2}+\varepsilon}\right)\left(\int_0^{P^{-k}}P^{2k+3}\mathrm{d}\beta+\int_{P^{-k}}|\beta|^{-\frac{2k+3}{k}}\mathrm{d}\beta\right)$$

$$=O(P^{k+3}Q^2(0)\mathrm{e}^{-c_8\sqrt{L}}).$$

**引理 3.8**

$$\sum_{M}\left(\int_0^1-\int_M\right)\left|\Im_0^{*2k+3}(\alpha,h,q)\Lambda^2\left(\frac{W_{h,q}}{\varphi(q)}\right)^{2m+4}\right|\mathrm{d}\alpha$$
$$=O(P^{k+3}Q^2(0)L^{-\sigma_0(1-3a)}).$$

**证明** 上式左端不超过

$$O\left(\sum_{q\leqslant L^{\sigma_0}}q\cdot Q^2(0)q^{-m-2}\cdot q^{-\frac{1}{2}(2k+3)}\int_{q^{-1}N^{-1}L^{\sigma_0}}|\beta|^{-\frac{2k+3}{k}}\mathrm{d}\beta\right)$$
$$=O(P^{k+3}Q^2(0)L^{-\sigma_0(1-3a)}).$$

**引理 3.9**

$$r'_{2k+2m+7}(N)=\Lambda^2\mathcal{S}(N)\Psi(N)+O(P^{k+3}L^{-\sigma}Q^2(0)),$$

其中

$$c_{13}P^{k+3}L^{-2k-2m-7}<\Psi(N)<c_{14}P^{k+3}L^{-2k-2m-7}.$$

**证明** 由引理 3.2,3.6,3.7 和 3.8, 可得

$$\begin{aligned}r'_{2k+2m+7}(N)&=\int_0^1\Im_0^{2k+3}(\alpha)\mathfrak{H}^2(\alpha)\mathrm{e}^{-2\pi\mathrm{i}N\alpha}\mathrm{d}\alpha\\&=\sum_{q\leqslant L^{\sigma_0}}\sum_{\substack{h=1\\(h,q)=1}}^{q}\Lambda^2\left(\frac{W_{h,q}}{\varphi(q)}\right)^{2k+2m+7}\\&\quad\times e_q(-Nh)\Psi(N)+O(P^{k+3}L^{-\sigma}Q^2(0)),\end{aligned}$$

其中

$$\Psi(N)=\sum_{n_1+\cdots+n_{2k+3}=N}\frac{1}{\prod_{i=1}^{2k+3}n_i^{1-a}\log n_i},$$

它显然满足引理中的不等式.

因为

$$\sum_{q>L^{\sigma_0}}\sum_{\substack{h=1\\(h,q)=1}}^{q}\left(\frac{W_{h,q}}{\varphi(q)}\right)^{2k+2m+7}e_q(-Nh)=O\left(\sum_{q>L^{\sigma_0}}q^{-k-m-2}\right)$$
$$=O(L^{-(k+m+1)\sigma_0}),$$

所以, 引理成立.

由引理 1.9 和 3.9, 可得定理.

# 附录：$K$ 的分布

定理中的同余条件是必不可少的，它不能用一个更弱的条件代替.

如果 $k$ 是一个奇数，则 $K=2$. 因此，我们有

**定理**　设 $k$ 是一个奇数. 每个充分大的奇数都可表作 $2k+2m+7$ 个素数的 $k$ 次幂之和. 每个充分大的整数都可表作至多 $2k+2m+8$ 个素数的 $k$ 次幂之和.

当 $k$ 为偶数时，$K$ 的分布是很不规律的，而且它的数值是非常大的. 为了说明这一点，我给出下面的一个表.

| $k$ | $K$ | $k$ | $K$ |
|---|---|---|---|
| 2 | $2^3\cdot 3$ | 52 | $2^4\cdot 3\cdot 5\cdot 53$ |
| 4 | $2^4\cdot 3\cdot 5$ | 54 | $2^3\cdot 3^4\cdot 7\cdot 19$ |
| 6 | $2^3\cdot 3^2\cdot 7$ | 56 | $2^5\cdot 3\cdot 5\cdot 29$ |
| 8 | $2^5\cdot 3\cdot 5$ | 58 | $2^3\cdot 3\cdot 59$ |
| 10 | $2^3\cdot 3\cdot 11$ | 60 | $2^4\cdot 3^2\cdot 5^2\cdot 7\cdot 11\cdot 13\cdot 31\cdot 61$ |
| 12 | $2^4\cdot 3^2\cdot 5\cdot 7\cdot 13$ | 62 | $2^3\cdot 3$ |
| 14 | $2^3\cdot 3$ | 64 | $2^8\cdot 3\cdot 5\cdot 17$ |
| 16 | $2^6\cdot 3\cdot 5\cdot 17$ | 66 | $2^3\cdot 3^2\cdot 7\cdot 23\cdot 67$ |
| 18 | $2^3\cdot 3^3\cdot 7\cdot 19$ | 68 | $2^4\cdot 3\cdot 5$ |
| 20 | $2^4\cdot 3\cdot 5^2\cdot 11$ | 70 | $2^3\cdot 3\cdot 11\cdot 71$ |
| 22 | $2^3\cdot 3\cdot 23$ | 72 | $2^5\cdot 3^3\cdot 5\cdot 7\cdot 13\cdot 19\cdot 37\cdot 73$ |
| 24 | $2^5\cdot 3^2\cdot 5\cdot 7\cdot 13$ | 74 | $2^3\cdot 3$ |
| 26 | $2^3\cdot 3$ | 76 | $2^4\cdot 3\cdot 5$ |
| 28 | $2^4\cdot 3\cdot 5\cdot 29$ | 78 | $2^3\cdot 3^2\cdot 7\cdot 79$ |
| 30 | $2^3\cdot 3^2\cdot 7\cdot 11\cdot 31$ | 80 | $2^6\cdot 3\cdot 5^2\cdot 11\cdot 17\cdot 41$ |
| 32 | $2^7\cdot 3\cdot 5\cdot 17$ | 82 | $2^3\cdot 3\cdot 83$ |
| 34 | $2^3\cdot 3$ | 84 | $2^4\cdot 3^2\cdot 5\cdot 7^2\cdot 13\cdot 29\cdot 43$ |
| 36 | $2^4\cdot 3^3\cdot 5\cdot 7\cdot 13\cdot 19\cdot 37$ | 86 | $2^3\cdot 3$ |
| 38 | $2^3\cdot 3$ | 88 | $2^5\cdot 3\cdot 5\cdot 23\cdot 89$ |
| 40 | $2^5\cdot 3\cdot 5^2\cdot 11\cdot 41$ | 90 | $2^3\cdot 3^3\cdot 7\cdot 11\cdot 19\cdot 31$ |
| 42 | $2^3\cdot 3^2\cdot 7^2\cdot 43$ | 92 | $2^4\cdot 3\cdot 5\cdot 47$ |
| 44 | $2^4\cdot 3\cdot 5\cdot 23$ | 94 | $2^3\cdot 3$ |
| 46 | $2^3\cdot 3\cdot 47$ | 96 | $2^7\cdot 3^2\cdot 5\cdot 7\cdot 13\cdot 17\cdot 97$ |
| 48 | $2^6\cdot 3^2\cdot 5\cdot 7\cdot 13\cdot 17$ | 98 | $2^3\cdot 3$ |
| 50 | $2^3\cdot 3\cdot 11$ | 100 | $2^4\cdot 3\cdot 5^3\cdot 11\cdot 101$ |

（贾朝华　译）

# 关于一个推广的华林问题 II[①]

华罗庚

## 引　言

设 $P(h)$ 是一个 $k$ 次整值多项式, 其首项系数为正. 令 $G(P(h))$ 为最小的正整数 $s$, 使得当整数 $N$ 充分大时, 丢番图方程

$$P(h_1)+\cdots+P(h_s)=N,\quad h_\nu\geqslant 0$$

总可解. 本文我们将证明

$$G(P(h))\leqslant 2^{k+1}(k-1),\tag{1}$$

这比我以前的结果[②]要好得多.

另一方面, 在 §4 中我们将证明: 当 $k\geqslant 5$, 而

$$P(h)=2^{k-1}F_k(h)-2^{k-2}F_{k-1}(h)+\cdots+(-1)^{k-1}F_1(h)$$

以及

$$F_i(h)=\frac{h(h-1)\cdots(h-i+1)}{i!}$$

时, 有

$$G(P(h))=\begin{cases}2^k-1, & \text{当 } k \text{ 为奇数时},\\ 2^k, & \text{当 } k \text{ 为偶数时}.\end{cases}\tag{2}$$

在华林问题的整个理论中, 仅有的能够确定 $G(P(h))$ 的定理是关于二次多项式的, 这就是

$$G(h^2)=4,\quad G\left(\frac{1}{2}(h^2-h)\right)=3.$$

有数值的证据支持这样的观点:

$$G(P(h))\leqslant\begin{cases}2^k-1, & \text{当 } k \text{ 为奇数时},\\ 2^k, & \text{当 } k \text{ 为偶数时}\end{cases}$$

---

① 1939 年 2 月 10 日收到. 发表于 *Journal of the Chinese Mathematical Society*, 1940, 2: 175–191.

② *Proc.London Math.Soc.*, 1937, 43: 161–182. 该文以后记为 I.

普遍地成立.

不失一般性, 我们可设 $P(h)$ 的常数项为零, 所有系数均为正.

§1. 设 $r(N)$ 为丢番图方程

$$N=P(x_1)+\cdots+P(x_s),\quad x_\nu\geqslant 0$$

的解数.

在文 I 和其他文章①中, 作者证明了下面的

**定理 1**　如果

$$s\geqslant\begin{cases}10k^3\log k, & \text{当 } k>15 \text{ 时},\\ 2^k+1, & \text{当 } 3\leqslant k\leqslant 15 \text{ 时},\end{cases}$$

则有

$$r(N)=a^{-\frac{s}{k}}\frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)}\mathcal{S}(N)N^{\frac{s}{k}-1}+O(N^{\frac{s}{k}-1-\rho}),$$

其中 $a$ 为 $P(x)$ 的首项系数, $\rho$ 是一个与 $N$ 无关的正数, $\mathcal{S}(N)$ 为文 I 中定义的奇异级数.

由此可见, 为了建立结果 (1), 我们只需证明: 当 $s\geqslant(k-1)2^{k+1}$ 时, 有

$$\mathcal{S}(N)\geqslant D>0, \tag{3}$$

其中 $D$ 是一个与 $N$ 无关的数.

令 $d$ 为 $P(h)$ 系数的最小公分母. 设 $p$ 是一个素数, $p^t\|d$, 而 $p^tP(h)=\Phi(h)$②. 于是, $\Phi(h)$ 系数的分母不能被 $p$ 整除. 令 $\theta^{(i)}$ 为最大的整数, 使得对于所有的 $h$, $\Phi(h)$ 的第 $i$ 阶导数满足

$$\Phi^{(i)}(h)\equiv 0(\mathrm{mod}\,p^{\theta^{(i)}})③,$$

而 $P^*(h)=p^{-\theta'}\Phi'(h)$. 令

$$\delta=\max_{1\leqslant i\leqslant k-1}(\theta^{(i)}-\theta^{(i+1)}),$$

以及

$$\gamma'=\begin{cases}\theta'+2-t+\delta, & \text{当 } p=2 \text{ 时},\\ \theta'+1-t+\delta, & \text{当 } p\neq 2 \text{ 时}.\end{cases}$$

① *J.Chinese Math.Soc.*, 1936, 1: 21–61; *Quar.J.Math.*, 1938, 9: 199–202.

② 这里的 $\Phi(h)$ 的定义与文 I 中的相差一个与 $p$ 互素的因子. 我们应将文 I 的引理 7.5 中的 $P_v^*(y)$ 改为 $\alpha_vP^*(y)$, 其中 $p\nmid\alpha_v$. 然而, 这对于讨论是非实质性的.

③ $\Phi(h)$ 不必是整系数的多项式. 因此, $\Phi^{(i)}(h)$ 可以不是整数. 然而, 在同余式 $\Phi^{(i)}(h)\equiv 0(\mathrm{mod}\,p^{\theta^{(i)}})$ 中, 它可以当作一个整数, 这是因为所有系数的分母都与 $p$ 互素.

# 賈榮懷

始遷祖蘭谷號紉之浙江紹興府上虞縣庠生由浙始遷江蘇之川沙廳

七世祖威字君復號方平明天啟辛酉科舉人

七世祖母氏吳

六世祖紹蘭字振儒由川沙始遷南滙之周浦

六世祖母氏朱

五世祖淞字右涓號鶴沙邑庠生例授

字吉甫號蓉卿行三嘉慶己巳年十月二十七日吉時生道光庚子科優貢江蘇松江府南滙縣廩膳生民籍

堂高伯祖棟　桓

堂曾伯叔祖長庚　長春　熙　長策

堂伯叔祖成炎　成林　景春　元照　景堃太學生　德培

堂叔履仁　履循　履鈺　周藩例贈登仕佐郎　應熊

應森　應杰　應龍　應銓國學生　應鉅　濱中太學

廩膳生

從堂兄弟昆明　昆法　昆秀　國珍　國琳　國琛

國根　國中　國芳　國惠　炳炎　國濟

由引理 1.1, 我们用文 I 的引理 7.6 中的方法, 可以推出

**引理 1.2** 如果 $l \geqslant 1+\gamma$, 则

$$N(p^t) = p^{s-1}N(p^{t-1}).$$

因而 (参见文 I 的 §7), 我们有

**定理 2** 如果存在一个整数 $s_0$, 使得对于所有的素数 $p$ 和所有的整数 $n$, 均有

$$N(s_0 \cdot P, p^{\gamma'}, n) > 0,$$

则当 $s \geqslant \max(s_0, 2k+1)$ 时, 我们有

$$\mathcal{S}(N) \geqslant D > 0.$$

由此可见, 为了证明 (1) 式, 我们只需对于 $s_0 \geqslant (k-1)2^{k+1}$ 证明

$$N(s_0 \cdot P, p^{\gamma'}, n) > 0 \tag{4}$$

即可. 这将在 §2 和 §3 中进行.

§2. **引理 2.1** (Davenport 和 Chowla)① 设 $\alpha_1, \cdots, \alpha_m$ 为 $m$ 个不同的剩余类 $\bmod h$, 而 $\beta_1, \cdots, \beta_n$ 为 $n$ 个不同的剩余类 $\bmod h$, 且 $(\beta_1, \cdots, \beta_n, h) = 1$. 则由

$$\alpha_i \text{ 或 } \alpha_i + \beta_j \quad (1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n)$$

所表出的不同剩余类的个数大于或等于 $\min(m+n, h)$.

**引理 2.2** 设 $P(x)$ 为 $k$ 次整系数多项式 $\bmod p$, 且 $\not\equiv P(0) (\bmod p)$. 如果 $p > k$, 则由 $P(x)$ 给出的不同值 $\bmod p$ 的个数大于或等于

$$\left[\frac{p}{k}\right] + 1.$$

**证明** 对于任意给定的整数 $a$, 同余式

$$P(x) \equiv a (\bmod p)$$

的解数至多为 $k$, 再由 $k \nmid p$ 立得引理.

**引理 2.3** 当 $s_0 \geqslant 2k$ 时, 对于所有的整数 $n$ 和 $p > k$, 有

$$N(s_0 \cdot P, p^{\gamma'}, n) > 0.$$

① 可见 Landau. Über einige neuere Fortschritte der additiven Zahlentheorie. *Cambridge Tract*, 第 8 页.

**证明** 因为 $p > k$, 所以, 此时 $\gamma' = 1$. 首先, 我们将要证明, 当 $s \geqslant 2k-1$ 时, 对于所有的整数 $n$, 同余式

$$\sum_{\nu=1}^{s} P(x_\nu) \equiv n(\mathrm{mod}p)$$

总可解. 对于 $p \leqslant 2k-1$, 这是显然的. 因而, 我们可设 $p > 2k-1$. 因为 $P(x)$ 给出至少 $\left[\frac{p}{k}\right]+1$ 个不同值 $\mathrm{mod}p$, 其中至少有 $\left[\frac{p}{k}\right]$ 个不能被 $p$ 整除, 又因为

$$\begin{aligned}\left[\frac{p}{k}\right]+1+(s-1)\left[\frac{p}{k}\right] &\geqslant s\left(\frac{p}{k}-1\right)+1\\ &\geqslant (2k-1)\left(\frac{p}{k}-1\right)+1\\ &= p+(k-1)\left(\frac{p}{k}-2\right) \geqslant p,\end{aligned}$$

所以, 由引理 2.1, 同余式对于所有的整数 $n$ 总可解.

其次①, 因为对于所有的 $x, P^*(x) \equiv 0(\mathrm{mod}p)$ 不能恒等地成立, 所以, 我们可取一个整数 $x'$ 使得 $P^*(x') \not\equiv 0(\mathrm{mod}p)$. 由证明的前一部分, 对于 $s \geqslant 2k-1$, 同余式

$$\sum_{\nu=1}^{s} P(x_\nu) \equiv n - P(x')(\mathrm{mod}p)$$

总可解. 因此, 我们可得引理.

§3. 本节中我们将使用以下约定的记号: 设 $Q(x)$ 为有理系数的多项式, $\alpha$ 为最大的整数, 使得 $Q(x)$ 系数的最小公分母可以被 $p^\alpha$ 整除, 那么

$$Q(x) \cong 0(\mathrm{mod}p^a)$$

表示对于所有的整数 $x$, 有

$$p^\alpha Q(x) \equiv 0(\mathrm{mod}p^{a+\alpha}),$$

这里 $a$ 可以是任意的整数. 例如

$$\frac{x^3-x}{3^7} \cong 0(\mathrm{mod}3^{-6}).$$

我们必须注意, "mod$p^0$" 不同于我们通常的记号 "mod1". 例如

$$\frac{x^3-x}{3\cdot 7} \equiv 0(\mathrm{mod}3^0),$$

① 本段中的讨论在引理 3.4 中不再重复.

但是

$$\frac{x^3-x}{3\cdot 7}\not\equiv 0(\mathrm{mod}1),$$

这是因为 $\frac{1}{7}$看作整数 mod3.

**引理 3.1**

$$Q(x)\cong 0(\mathrm{mod}p^a)$$

成立的充分必要条件是

$$Q(x)=a_1F_k(x)+\cdots+a_kF_1(x),\quad p^a|(a_1\cdots,a_k),$$

这里 $F_i(x)$ 如引言中所定义.

通过考虑 $p^\alpha Q(x)$, 容易证明本引理.

**引理 3.2** 令 $a$ 为最大的整数使得

$$Q(x)\cong 0(\mathrm{mod}p^a).$$

如果

$$Q'(x)\cong 0(\mathrm{mod}p^b),$$

则

$$b-a\leqslant\left[\frac{k}{p-1}\right]-1.$$

**证明** 如果我们用 $p^tQ(x)$ 代替 $Q(x)$, 则 $b-a$ 不变, 因而, 不失一般性, 我们总可设 $a=0$, 即在引理 3.1 中有

$$p^0|(a_1,\cdots,a_k),\quad p\nmid(a_1,\cdots,a_k)$$

(上式表明, 所有的 $a_i$ 在其即约形式中的分母都与 $p$ 互素). 记

$$Q'(x)=b_1F_{k-1}(x)+b_2F_{k-2}(x)+\cdots+b_{k-1}F_1(x)+b_k.$$

令 $\Delta^i(P(x))$ 为 $P(x)$ 的 $i$ 阶差分, 则

$$\begin{aligned}
b_1&=\Delta^{k-1}Q'(x)=(\Delta^{k-1}Q(x))'=a_1,\\
b_2&=(\Delta^{k-2}Q'(x))_{x=0}=(\Delta^{k-2}Q(x))'_{x=0}=-\frac{a_1}{2}+a_2,\\
&\cdots\cdots\\
b_k&=(Q'(x))_{x=0}=(-1)^k\left(\frac{a_1}{k}-\frac{a_2}{k-1}+\frac{a_3}{k-2}-\cdots+(-1)^ka_k\right).
\end{aligned}$$

从假设和引理 3.1, 我们可得

$$p^b|(b_1,\cdots,b_k).$$

如果 $b > [k/(p-1)]-1$, 则

$$\begin{aligned}&p^b|(a_1,a_2,\cdots,a_{p-1}),\\&p^{b-1}|(a_p,a_{p+1},\cdots,a_{2p-2}),\\&p^{b-2}|(a_{2p-1},\cdots),\\&\qquad\qquad\cdots\cdots\\&p|p^{b-([k/(p-1)]-1)}|(a_{([k/(p-1)]-1)(p-1)+1},\cdots,a_k).\end{aligned}$$

这就是说, 有 $p|(a_1,\cdots,a_k)$, 但这是一个矛盾.

**引理 3.3** 如果 $p=2$, 则

$$p^{\gamma'}\leqslant(k-1)2^{k+1};$$

如果 $p>2$, 则

$$p^{\gamma'}\leqslant(k-1)p^{[k/(p-1)]}<(k-1)2^{k+1}.$$

**证明** 由文 I 中的引理 7.4, 我们有

$$p^{\delta}\leqslant k-1.$$

与引理 3.2 相关联, 当 $p=2$ 时, 有

$$p^{\gamma'}=p^{\theta'-t+2+\delta}\leqslant(k-1)2^{k+1};$$

而当 $p>2$ 时, 有

$$p^{\gamma'}\leqslant(k-1)p^{[k/(p-1)]}.$$

因此, 我们可得

**引理 3.4** 如果 $s\geqslant(k-1)2^{k+1}-1$, 且 $P(x)\not\equiv 0(\bmod p)$, 则对于所有的整数 $n$, 同余式

$$\sum_{\nu=1}^{s}P(x_\nu)\equiv n(\bmod p^{\gamma'})$$

可解. 因此, 当 $s\geqslant(k-1)2^{k+1}$ 时, 对于所有的整数 $n$ 和素数 $p$, 我们有

$$N(s_0\cdot P,p^{\gamma'},n)>0.$$

因此, (4) 式成立. 再由定理 1 和 2, 我们有

**定理 3** 如果 $P(x)$ 是一个 $k$ 次整值多项式, 其首项系数为正, 且对于任意素数 $p$, $P(x)$ 不恒等地同余于 $P(0)\bmod p$, 则有

$$G(P(x))\leqslant(k-1)2^{k+1}.$$

§4. 本节我们将考虑特殊的多项式

$$H_k(x)=2^{k-1}F_k(x)-2^{k-2}F_{k-1}(x)+\cdots+(-1)^{k-1}F_1(x).$$

**引理 4.1**　设 $\tau$ 为满足 $2^\tau||k!$ 的整数, $\sigma$ 为满足 $2^\sigma\leqslant k<2^{\sigma+1}$ 的整数. 用 $M$ 表示这样的整数集合, 它由 $k-2$ 个整数的乘积的全体所组成, 这里 $k-2$ 个整数取自任意 $k$ 个连续的整数. 则 $M$ 中的每个元素都能被 $2^{\tau-2\sigma+1}$ 整除.

**证明**　首先, 我们考虑 $M$ 中的一部分元素, 它们对应的 $k$ 个连续整数中有一个为 0. 我们只需证明:

(i) 如果 e 和 $k-1-\mathrm{e}$ 都 $<2^\sigma$, 则

$$2^{-\sigma+1}\mathrm{e}!(k-1-\mathrm{e})!$$

可以被 $2^{\tau-2\sigma+1}$ 整除;

(ii) 如果 e 或者 $k-1-\mathrm{e}\geqslant 2^\sigma$, 则

$$2^{-\sigma}\mathrm{e}!(k-1-\mathrm{e})!$$

可以被 $2^{\tau-2\sigma+1}$ 整除. 显然, (i) 和 (ii) 可用公式表示如下:

(i) $\displaystyle\sum_{\lambda=1}^{\infty}\left(\left[\frac{k}{2^\lambda}\right]-\left[\frac{\mathrm{e}}{2^\lambda}\right]-\left[\frac{k-1-\mathrm{e}}{2^\lambda}\right]\right)\leqslant\sigma;$

(ii) 如果 $2^{\sigma+1}>\mathrm{e}\geqslant 2^\sigma$(我们可以不失一般性地假设), 则

$$\sum_{\lambda=1}^{\infty}\left(\left[\frac{k}{2^\lambda}\right]-\left[\frac{\mathrm{e}}{2^\lambda}\right]-\left[\frac{k-1-\mathrm{e}}{2^\lambda}\right]\right)\leqslant\sigma-1.$$

我们仅给出 (ii) 的证明, 用相同的讨论容易得到 (i).

显然, 有

$$\sum_{\lambda=\sigma}^{\infty}\left(\left[\frac{k}{2^\lambda}\right]-\left[\frac{\mathrm{e}}{2^\lambda}\right]-\left[\frac{k-1-\mathrm{e}}{2^\lambda}\right]\right)=0.$$

设 $2^d||k$. 如果 $\lambda>d$, 则

$$\left[\frac{k}{2^\lambda}\right]-\left[\frac{\mathrm{e}}{2^\lambda}\right]-\left[\frac{k-1-\mathrm{e}}{2^\lambda}\right]$$

$$<\frac{k-1}{2^\lambda}-\left(\frac{\mathrm{e}}{2^\lambda}-1\right)-\left(\frac{k-1-\mathrm{e}}{2^\lambda}-1\right)=2,$$

因而

$$\left[\frac{k}{2^\lambda}\right]-\left[\frac{\mathrm{e}}{2^\lambda}\right]-\left[\frac{k-1-\mathrm{e}}{2^\lambda}\right]\leqslant 1.$$

如果 $\lambda \leqslant d$, 我们记 $k=2^d k_0$, 以及

$$\mathrm{e}=2^d e_0+2^{d-1}e_1+\cdots+e_d,\quad 0\leqslant e_i\leqslant 1,\quad i=1,2,\cdots,d.$$

则有

$$k-1-\mathrm{e}=2^d(k_0-e_0-1)+2^{d-1}(1-e_1)+\cdots+(1-e_d).$$

易见

$$\left[\frac{k}{2^\lambda}\right]-\left[\frac{\mathrm{e}}{2^\lambda}\right]-\left[\frac{k-1-\mathrm{e}}{2^\lambda}\right]\leqslant\sigma.$$

因此

$$\sum_{\lambda=1}^{\infty}\left(\left[\frac{k}{2^\lambda}\right]-\left[\frac{\mathrm{e}}{2^\lambda}\right]-\left[\frac{k-1-\mathrm{e}}{2^\lambda}\right]\right)\leqslant\sigma-1.$$

其次, 我们考虑 $M$ 中取自连续整数

$$a+1,a+2,\cdots,a+k \tag{A}$$

的元素. 令 $\Lambda$ 为 (A) 中含有 2 的最大幂次者 (容易验证 $\Lambda$ 是唯一的), 构成集合

$$a+1-\Lambda,a+2-\Lambda,\cdots,a+k-\Lambda. \tag{B}$$

(A) 中任一项的 2 的幂次等于 (B) 中对应项的 2 的幂次, 唯一的例外是当 $\Lambda$ 对应于 0 时. $M$ 中取自 (A) 的最不利的元素是

$$\frac{(a+1)(a+2)\cdots(a+k)}{\Lambda\cdot\Lambda_1},$$

其中 $\Lambda_1$ 为 (A) 中含有 2 的第二高次幂者. 上述的元素所含 2 的幂次等于

$$\frac{(\Lambda-(a+1))!(a+k-\Lambda)!}{\Lambda_1\cdot\Lambda}$$

中所含的 2 的幂次. 再用第一部分中的证明, 我们可以完成引理的证明.

**引理 4.2** 令

$$K_k(x)=x(x-1)\cdots(x-k+1).$$

则 $K_k(x)$ 是一个剩余多项式 $\mathrm{mod}2^{\tau-\sigma}$, $K_k''(x)$ 是一个剩余多项式 $\mathrm{mod}2^{\tau-2\sigma+1}$.

**证明** 由引理 4.1 可立得第二个结论, 而用相同的讨论易得第一个结论.

**引理 4.3** 存在整数 $x_1$, 使得

$$K_k(x_1)\equiv 0(\mathrm{mod}2^{\tau+1})$$

以及

$$2^{\tau-\sigma+1} \nmid K_k'(x_1).$$

又有整数 $x_2$, 使得

$$K_k(x_2) \equiv 2^\tau (\mathrm{mod} 2^{\tau+1})$$

以及

$$2^{\tau-\sigma+1} \nmid K_k'(x_2).$$

**证明**　取 $x_1 = 2^\sigma$. 则有 $K_k(x_1) = 0$, 和

$$K_k'(x_1) = 2^{-\sigma} k!,$$

它不能被 $2^{\tau-\sigma+1}$ 整除.

再取 $x_2 = k$. 则有

$$K_k(x_2) = k! \equiv 2^\tau (\mathrm{mod} 2^{\tau+1})$$

和

$$K_k'(x_2) \equiv 2^{-\sigma} k!\ (\mathrm{mod} 2^{\tau-\sigma+1}).$$

**定理 4**　令

$$k! F_k(x) = K_k(x).$$

则

$$F_k(x) \equiv a (\mathrm{mod} 2^l), \quad 2^{\tau-\sigma+1} \nmid K_k'(x)$$

对于所有的 $a$ 和 $l(>0)$ 均可解.

**证明**　由引理 4.3 知, 对于 $l=1$, 定理是显然的. 我们将用归纳法. 令 $x_1$ 为整数, 使得

$$K_k(x_1) \equiv k! a (\mathrm{mod} 2^{l+\tau}), \quad 2^{\tau-\sigma+1} \nmid K_k'(x_1).$$

对于 $l \geqslant 1$, 由引理 1.1 中相同的方法, 有

$$K_k(x + 2^{l+\sigma} y) \equiv K_k(x) + 2^{l+\sigma} y K_k'(x) (\mathrm{mod} 2^{l+\tau+1})$$

和

$$K_k'(x + 2^{l+\sigma} y) \equiv K_k'(x) (\mathrm{mod} 2^{\tau-\sigma+1}).$$

因此, 我们可以找到一个 $y$, 使得

$$K_k(x_1 + 2^{l+\sigma} y) \equiv k! a (\mathrm{mod} 2^{l+\tau+1}),$$

以及

$$2^{\tau-\sigma+1} \nmid K'_k(x_1 + 2^{l+\sigma}y).$$

**引理 4.4**

$$H_k(y+1) + H_k(y) = 2^k F_k(y) + (-1)^{k+1}.$$

**证明** 当 $k=1$ 时, 引理是显然的. 由归纳法, 以及

$$H_k(y) = 2^{k-1}F_k(y) - H_{k-1}(y),$$

可得结论.

因而, 有

**引理 4.5**

$$H_k(y+2) - H_k(y) = 2^k F_{k-1}(y).$$

**定理 5**

$$G(H_k(x)) \geqslant \begin{cases} 2^k - 1, & \text{当 } k \text{ 为奇数时}, \\ 2^k, & \text{当 } k \text{ 为偶数时}. \end{cases}$$

**证明** 由引理 4.5 知, $H_k(x)$ 仅给出两个不同的值, 0 和 $(-1)^{k-1}(\bmod 2^k)$. 因此,

$$G(H_k(x)) \geqslant 2^k - 1.$$

此外, 如果 $k$ 为偶数, 则由引理 4.5 可知, $H_k(x)$ 仅给出三个不同的值, $0, (-1)^{k-1}$ 和 $(-1)^{k-1} + 2^k(\bmod 2^{k+1})$. 同余式

$$\sum_{\nu=1}^{2^k-1} H_k(h_\nu) \equiv 2^k(\bmod 2^{k+1})$$

无解, 所以

$$G(H_k(x)) \geqslant 2^k.$$

现在我们来证明

$$G(H_k(x)) \leqslant \begin{cases} 2^k - 1, & \text{当 } k \text{ 为奇数时}, \\ 2^k, & \text{当 } k \text{ 为偶数时}. \end{cases}$$

用与 §1 中相同的讨论, 我们仅需对于

$$s_0 = \begin{cases} 2^k - 1, & \text{当 } k \text{ 为奇数时}, \\ 2^k, & \text{当 } k \text{ 为偶数时}, \end{cases}$$

证明

$$N(s_0 \cdot H_k, p^{\gamma'}, n) > 0$$

即可.

情形 I. $k$ 为奇数.

我们定义

$$E_k(y) = 2^{-k}H_k(2y) \text{ 和 } O_k(y) = 2^{-k}(H_k(2y+1)-1).$$

**引理 4.6**　我们有

$$E_k(y) \not\equiv E_k(0) \text{ 和 } O_k(y) \not\equiv O_k(0) (\bmod 2).$$

**证明**　1) 由引理 4.5, 因为 $F_{k-1}(k-1)=1$, 所以, 我们有

$$E_k(y+1) - E_k(y) = F_{k-1}(2y),$$

引理的第一部分得证.

2) 相似地, 我们有

$$O_k(y+1) - O_k(y) = F_{k-1}(2y+1).$$

因为 $F_{k-1}(k)=k$, 所以, 可得引理的第二部分.

**引理 4.7**　设 $p=2$. 则 $E_k(x)$ 的 $\gamma' \leqslant 3$(见 §1 中的定义).

**证明**　因为 $\delta \leqslant \sigma$ 和

$$\gamma' = \theta - t + \delta + 2 \leqslant \tau - \sigma + 1 - \tau + \sigma + 2 = 3,$$

所以, 只需证明 $2^{\tau}E_k'(x)$ 不是剩余多项式 $\bmod 2^{\tau-\sigma+2}$ 即可.

如若不然, 我们会有

$$2^{\tau}(E_k'(y+2) - E_k'(y)) = 2^{\tau+1}F_{k-1}'(2y) \cong 0 (\bmod 2^{\tau-\sigma+2}),$$

而

$$2^{\tau-\sigma+2} \nmid 2^{\tau+1}F_{k-1}'(k-1).$$

**引理 4.8**　设 $p=2$. 则 $O_k(x)$ 的 $\gamma' \leqslant 3$.

本引理的证明与引理 4.7 的证明相似, 其中最后一行要代之以

$$2^{\tau-\sigma+2} \nmid 2^{\tau+1}F_{k-1}'(k).$$

**引理 4.9** 如果 $k \geqslant 5, s \geqslant 2^k - 1$, 则对于所有的 $n$ 有

$$N(s \cdot H_k, 2^{\gamma'}, n) > 0.$$

**证明** 令 $n'$ 为满足

$$n \equiv n'(\mathrm{mod} 2^k), \quad 0 \leqslant n' < 2^k$$

的整数. 由引理 4.7 和 4.8($2^{\gamma'} \leqslant 8$) 知, 对于所有的整数 $n$ 和 $l(> 0)$, 同余式

$$\sum_{\nu=1}^{n'} O_k(x_\nu) + \sum_{\nu=n'+1}^{2^k-1} E_k(x_\nu) \equiv m(\mathrm{mod} 2^l)$$
$$(2 \text{ 不能整除 } O_k^*(x_\nu) \text{ 或者 } E_k^*(x_\nu) \text{ 中的一个})$$

有解. 因此, 对于所有的整数 $n$, 同余式

$$\sum_{\nu=1}^{2^k-1} H_k(x_\nu) \equiv n(\mathrm{mod} 2^{\gamma'}), \quad (2 \text{ 不能整除 } H_k^*(x_\nu) \text{ 中的一个})$$

可解.

**引理 4.10** 如果 $s \geqslant 2^k - 1, k > 15$, 则对于所有的整数 $n$ 和素数 $p$, 有

$$N(s \cdot H_k, p^{\gamma'}, n) > 0.$$

**证明** 1) 如果 $p > k$, 这在引理 2.3 中已经证明过了.

2) 如果 $k \geqslant p > 2$, 则对于 $k > 15$, 由引理 3.3 和不等式

$$p^{\gamma'} \leqslant (k-1)p^{[k/(p-1)]} \leqslant (k-1)3^{[1/2k]} < 2^k - 1,$$

可得引理.

3) 如果 $p = 2$, 这在引理 4.9 中已经证明过了.

由定理 1 和 2, 对于奇数 $k > 15$, 我们可得

$$G(H_k(x)) \leqslant 2^k - 1.$$

因此, 我们有

**定理 6** 如果 $k(> 15)$ 是一个奇数, 则

$$G(H_k(x)) = 2^k - 1.$$

情形 II. $k$ 为偶数.

**引理 4.11**　如果 $s \geqslant 2^k, k \geqslant 6$, 则有

$$N(s \cdot H_k, 2^{\gamma'}, n) > 0.$$

**证明**　令 $n'$ 为满足

$$n \equiv (-1)^{k-1} n' (\bmod 2^k), \quad 0 < n' \leqslant 2^k$$

的整数.

1) $n' > 8$. $O_k(x)$ 如情形 I 中所定义. 由引理 4.8(它对于偶数 $k$ 也成立) 知, 对于所有的整数 $m$ 和 $l(> 0)$, 同余式

$$\sum_{\nu=1}^{n'} O_k(x_\nu) \equiv m (\bmod 2^l) \quad (2 \text{ 不能整除 } O_k^*(x_\nu) \text{ 中的一个})$$

可解. 因此, 对于所有的整数 $n$, 同余式

$$\sum_{\nu=1}^{2^k} H_k(x_\nu) \equiv n (\bmod 2^{\gamma'}) \quad (2 \text{ 不能整除 } H_k^*(x_\nu) \text{ 中的一个})$$

可解.

2) $n' \leqslant 8$. 由引理 4.4 和定理 4 知, 对于所有的整数 $m$ 和 $l(> 0)$, 同余式

$$\sum_{\nu=2}^{n'} O_k(x_\nu) + 2^{-k}(H_k(x+1) + H_k(x)) \equiv m (\bmod 2^k)$$

可解. 再由 $9 < 2^k$ 可得引理.

**引理 4.12**　如果 $k > 16, s \geqslant 2^k$. 则对于所有的整数 $n$ 和所有的素数 $p$, 有

$$N(s \cdot H_k, p^{\gamma'}, n) > 0.$$

本引理的证明与引理 4.10 的证明相同.

因此, 我们有

**定理 7**　如果 $k(> 16)$ 是一个偶数, 则

$$G(H_k(x)) = 2^k.$$

附：1939 年 3 月 5 日添加的注记.

证明的分析部分可以大大地改进. 例如, 将本文的算术结果结合起来, 我们可以得到

$$G\left(\frac{1}{k!} x(x-1) \cdots (x-k+1)\right) \leqslant 2k + 2m + 5,$$

其中

$$m = \left[ \frac{\log\frac{b}{2} + \log\left(1 - \frac{2}{k}\right)}{\log k - \log(k-1)} \right],$$

而

$$b = \begin{cases} k^3(\log k + 1.25\log\log k^2), & \text{当 } k \geqslant 15 \text{ 时}, \\ 2^{k-1}, & \text{当 } k < 15 \text{ 时}. \end{cases}$$

进一步地, 定理 6 和 7 对于 $k \geqslant 4$ 也成立.

(贾朝华　译)

# 关于三次多项式的华林问题[①]

华罗庚 (中国, 国立清华大学)

假设一个三次整值多项式可以表作

$$P(x)=\frac{1}{6}a(x^3-x)+\frac{1}{2}b(x^2-x)+cx+d,$$

其中 $a,b,c,d$ 为整数, $(a,b,c)=1, a>0$. 本文的目的是要证明: 对于充分大的整数 $N$, 丢番图方程

$$P(x_1)+\cdots+P(x_8)=N,\quad x_\nu\geqslant 0$$

总可解. 这个结果要好过我以前的结果, 那时我们需要 9 个 $P(x)(x\geqslant 0)$ 的值.

## 1. 记　　号

设 $N$ 为充分大的整数, 即 $N\geqslant c_1$, 这里的 $c_1$ 和以后的 $c_2,\cdots$ 均表示只依赖于 $P(x)$ 系数的正数. 令 $2P$ 为 $P(x)=N$ 的最大正根. 它存在且为正, 并随 $N$ 趋向无穷.

设 $d$ 为 $P(x)$ 系数的最小公分母, $q$ 为一个正整数. 设

$$q^*=(q,d)q,\quad e(x)=\mathrm{e}^{2\pi\mathrm{i}x},$$

$$S_{a,q}=\sum_{h=1}^{q^*}e\left(\frac{a}{q}P(h)\right),$$

$$A(q)=\sum_{\substack{a=1\\(a,q)=1}}^{q}\left(\frac{S_{a,q}}{q^*}\right)^7 e\left(-\frac{a}{q}n\right),$$

$$\mathcal{S}(n)=\sum_{q=1}^{\infty}A(q),\quad \mathcal{S}'(n)=\sum_{q\leqslant P^{\frac{8}{9}}}A(q).$$

---

① 1940 年 6 月 25 日收到 (本文在二战之前曾寄到*Acta Arith.*). 发表于 *Journal of Indian Mathematical Society, New Series*, 1940, 4(4): 127–135.

又设

$$T(\alpha)=T(\alpha,P)=\sum_{P\leqslant\mu\leqslant 2P}e(P(\mu)\alpha),$$

$$T_1(\alpha)=T(\alpha,P^{\frac{4}{5}}),$$

$$T^7(\alpha)T_1(\alpha)=\sum_n r_8'(n)e(n\alpha),$$

$$I(\beta)=\int_P^{2P}e\left(\frac{1}{6}\beta a v^3\right)\mathrm{d}v.$$

我们用 $\varepsilon$ 表示一个任意小的正数.

我们按通常的方式, 将区间 $0\leqslant\alpha\leqslant 1$ 分成属于所有有理点 $\frac{a}{q}$的 Farey 弧, 这里 $1\leqslant q\leqslant P^{2-\varepsilon}, 0\leqslant a\leqslant q, (a,q)=1$. 我们再将这些弧分成优弧 $M(1\leqslant q\leqslant P^{1+\varepsilon})$ 和劣弧 $m(P^{1+\varepsilon}<q\leqslant P^{2-\varepsilon})$. 在两种情形里, 弧均有形式

$$\alpha=\frac{a}{q}+\beta,\quad -\frac{\theta_1}{qP^{2-\varepsilon}}\leqslant\beta\leqslant\frac{\theta_2}{qP^{2-\varepsilon}},$$

其中

$$\frac{1}{2}\leqslant\theta_1\leqslant 1,\quad \frac{1}{2}\leqslant\theta_2\leqslant 1.$$

进一步地, 我们将优弧分成 $M_1(1\leqslant q\leqslant P^{\frac{8}{9}})$ 和 $M_2(P^{\frac{8}{9}}<q\leqslant P^{1+\varepsilon})$.

为了避免重复许多熟知的讨论, 我们将经常参考我以前的两篇文章①.

## 2. 劣　　弧

**引理 1**②

$$\int_0^1|T(\alpha)|^6\mathrm{d}\alpha=O(P^{6-2-\frac{1}{2}+\varepsilon}).$$

**引理 2**

$$\int_0^1|T^2(\alpha)T_1^4(\alpha)|\mathrm{d}\alpha=O(P^{1+\frac{8}{5}+\varepsilon}).$$

本引理的证明与 Davenport③关于 $P(x)=x^3$ 的证明相似.

**引理 3**

$$\int_0^1|T^5(\alpha)T_1(\alpha)|\mathrm{d}\alpha=O(P^{5+\frac{4}{5}-2-\frac{1}{2}-\frac{1}{40}+\varepsilon}).$$

① On a generalized Waring problem. *Proc.London Math.Soc.*, 1937, 43: 161–182;On Waring's problem for fifth powers. *Proc.London Math.Soc.*, 1939, 45: 144–160. 它们将被分别记做 I 和 II.

② Hua. *Quarterly Jour.*, 1938, 9: 199–202.

③ Davenport,C.R., 1938, 207: 1366.

**证明**　由 Hölder 不等式, 引理 1 和 2, 我们有

$$\begin{aligned}&\int_0^1 |T^5(\alpha)T_1(\alpha)|\mathrm{d}\alpha\\ =&\int_0^1 |T(\alpha)|^{\frac{9}{2}}|T(\alpha)|^{\frac{1}{2}}|T_1(\alpha)|\mathrm{d}\alpha\\ \leqslant&\left(\int_0^1 |T(\alpha)|^{\frac{9}{2}\cdot\frac{4}{3}}\mathrm{d}\alpha\right)^{\frac{3}{4}}\left(\int_0^1 |T(\alpha)|^2|T_1(\alpha)|^4\mathrm{d}\alpha\right)^{\frac{1}{4}}\\ =&O(P^{\frac{3}{4}(6-\frac{5}{2})+\frac{1}{4}(1+\frac{8}{5})+\varepsilon}).\end{aligned}$$

**引理 4**

$$\sum_m\int_m |T^7(\alpha)T_1(\alpha)|\mathrm{d}\alpha=O(P^{5+\frac{4}{5}-3-\frac{1}{40}+\varepsilon}).$$

**证明**　由熟知的讨论[①], 在 $m$ 上, 我们有

$$T(\alpha)=O(P^{\frac{3}{4}+\varepsilon}).$$

因此

$$\begin{aligned}&\sum_m\int_m |T^7(\alpha)T_1(\alpha)|\mathrm{d}\alpha\\ =&O(P^{\frac{3}{2}+\varepsilon}\int_0^1 |T^5(\alpha)T_1(\alpha)|\mathrm{d}\alpha)\\ =&O(P^{5+\frac{4}{5}-3-\frac{1}{40}+\varepsilon}).\end{aligned}$$

## 3. 优　弧

**引理 5**　如果 $|\beta|\leqslant\dfrac{1}{2}$, 则

$$q^{*-1}S_{a,q}I(\beta)=(q^{-\frac{1}{3}+\varepsilon}\min[P,|\beta|^{-\frac{1}{3}}]).$$

**证明**　由文 II 的引理 2.7 和估计

$$S_{a,q}=O(q^{\frac{2}{3}+\varepsilon}),$$

可得结论.

**引理 6**[②]　如果 $\alpha=\dfrac{a}{q}+\beta, q\leqslant P^{1+\varepsilon}, |\beta|\leqslant q^{-1}P^{-2-\varepsilon}$, 则有

$$I(\alpha)-q^{*-1}S_{a,q}I(\beta)=O(q^{\frac{3}{4}+\varepsilon}).$$

---

① 可见 Gebbcke, 定理 10, *Math.Annalen*, 1931, 105: 637–652.

② 按照我目前关于指数和的工作 (将发表在*Chinese J.Math.* 第二卷上), 我们可以改进引理 6, 从而没有必要再划分 $M_1$ 和 $M_2$. 但为了便于读者阅读起见, 我仍采用目前的形式.

这是文 II 的引理 3.2.

**引理 7**

$$\sum_{M_2}\int_{M_2}|T^7(\alpha)T_1(\alpha)|\mathrm{d}\alpha=O(P^{5+\frac{4}{5}-3-\frac{1}{40}+\varepsilon}).$$

**证明** 由引理 5 和 6 知

$$T(\alpha)=O(q^{\frac{3}{4}+\varepsilon})+O(q^{-\frac{1}{3}+\varepsilon}P)=O(P^{\frac{3}{4}+\varepsilon}).$$

余下的证明与引理 4 中的相似.

**引理 8**

$$\sum_{M_1}\int_{M_1}|T^7(\alpha)-q^{*-7}S_{a,q}^7I^7(\beta)|\mathrm{d}\beta=O(P^{4-\frac{1}{3}+\varepsilon}).$$

**证明** 由引理 5 和 6, 我们有

$$|T^7(\alpha)-q^{*-7}S_{a,q}^7I^7(\beta)|=O(q^{\frac{3}{4}+\varepsilon}q^{-2}\min[P^6,|\beta|^{-2}]),$$

这里用到了

$$q^{\frac{3}{4}+\varepsilon}\leqslant\begin{cases}q^{-\frac{1}{3}+\varepsilon}P^{\frac{13}{12}\cdot\frac{8}{9}}\leqslant q^{-\frac{1}{3}+\varepsilon}P,\\ P^{\frac{3}{4}\cdot\frac{8}{9}+\varepsilon}=P^{\frac{2}{3}+\varepsilon}\leqslant q^{-\frac{1}{3}+\varepsilon}|\beta|^{-\frac{1}{3}}.\end{cases}$$

因此, 引理中等式的左边不超过

$$O\left[\sum_{q\leqslant P^{\frac{8}{9}}}q\cdot q^{\frac{3}{4}+\varepsilon}q^{-2}\left(\int_0^{P^{-3}}P^6\mathrm{d}\beta+\int_{P^{-3}}|\beta|^{-2}\mathrm{d}\beta\right)\right]$$

$$=O\left(P^3\sum_{q\leqslant P^{\frac{8}{9}}}q^{-\frac{1}{4}}\right)=O\left(P^{4-\frac{1}{3}+\varepsilon}\right).$$

**引理 9**

$$\sum_{M_1}\int_{\overline{M}_1}|q^{*-7}S_{a,q}^7I^7(\beta)|\mathrm{d}\beta=O(P^{4-\frac{4}{9}+\varepsilon}),$$

这里 $\overline{M}_1$ 是 $M_1$ 在 $(-\infty,\infty)$ 中的余集.

**证明** 左边不超过

$$O\left(\sum_{q\leqslant P^{\frac{8}{9}}}q\cdot q^{-\frac{7}{3}+\varepsilon}\int_{q^{-1}P^{-2+\varepsilon}}|\beta|^{-\frac{7}{3}}\mathrm{d}\beta\right)$$

$$=O\left(P^{\frac{8}{3}}\sum_{q\leqslant P^{\frac{8}{9}}}q\cdot q^{-\frac{7}{3}}q^{\frac{4}{3}+\varepsilon}\right)$$

$$= O\left(P^{\frac{8}{3}+\frac{8}{9}+\varepsilon}\right) = O(P^{4-\frac{4}{9}+\varepsilon}).$$

**引理 10**　令

$$F(n) = \int_{-\infty}^{\infty} I^7(\beta)\mathrm{e}^{-2\pi i n\beta}\mathrm{d}\beta.$$

如果 $\frac{1}{10}N \leqslant n \leqslant N$, 则有

$$c_2P^4 \leqslant F(n) \leqslant c_3P^4.$$

**证明**　我们有

$$F(n) = \int_{-\infty}^{\infty}\left(\int_P^{2P} e\left(\frac{1}{6}ax^3\beta\right)\mathrm{d}x\right)^7 e(-n\beta)\mathrm{d}\beta$$
$$= (2P)^4\int_{-\infty}^{\infty}\left(\int_{\frac{1}{2}}^{1} e(x^3\beta)\mathrm{d}x\right)^7 e(-c\beta)\mathrm{d}\beta,$$

其中 $0 < c \leqslant 1+\varepsilon$. 如文 II 的引理 1.8 中所示, 我们可以证明

$$\int_{-\infty}^{\infty}\left(\int_{\frac{1}{2}}^{1} e(x^3\beta)\mathrm{d}x\right)^7 e(-c\beta)\mathrm{d}\beta \geqslant c_4.$$

**引理 11**

$$\sum_{M_1}\int_{M_1} T^7(\alpha)e(-n\alpha)\mathrm{d}\alpha = F(n)\mathcal{S}'(n) + O(P^{4-\frac{1}{3}+\varepsilon}).$$

**证明**　由引理 8,9 和 10, 我们有

$$\sum_{M_1}\int_{M_1} T^7(\alpha)e(-n\alpha)\mathrm{d}\alpha$$
$$= \sum_{M_1} q^{*-7}S_{a,q}^7 e\left(-\frac{na}{q}\right)$$
$$\times\int_{-\infty}^{\infty} I^7(\beta)e(-n\beta)\mathrm{d}\beta + O(P^{4-\frac{1}{3}+\varepsilon})$$
$$= F(n)\mathcal{S}'(n) + O(P^{4-\frac{1}{3}+\varepsilon}).$$

## 4. 奇 异 级 数

令 $d$ 表示 $P(x)$ 系数的最小公分母, $dP(x) = \phi(x)$. 令 $p$ 表示素数, $p^t \| d$. 又令 $\theta$ 为 $p$ 的最高次幂, 使得对于所有的 $x$, 均有 $\phi'(x) \equiv 0(\bmod p^\theta)$. 设 $P^*(x) = p^{-\theta}\phi'(x)$.

设

$$\gamma = \begin{cases} \theta + 3 - t, & \text{当 } p = 2 \text{ 时}, \\ \theta + 1 - t, & \text{当 } p > 2 \text{ 时}. \end{cases}$$

设 $N(n, p^\gamma)$ 为同余式

$$P(x_1) + \cdots + P(x_7) \equiv n(\mathrm{mod} p^\gamma)$$
$$(0 \leqslant x_i \leqslant p^\gamma, p \nmid \{P^*(x_1), \cdots, P^*(x_7)\})$$

的解数.

**引理 12** 如果对于所有的整数 $n$ 和所有的素数 $p$, 均有 $N(n, p^\gamma) > 0$, 则

$$\mathcal{S}(n) \geqslant c_5 > 0.$$

这是文 I 的引理 7.9.

**引理 13** (Davenport 和 Chowla)[①] 设 $\alpha_1, \cdots, \alpha_m$ 为 $m$ 个不同的剩余类 $\mathrm{mod} h$, $\beta_1, \cdots, \beta_n$ 为 $n$ 个不同的剩余类 $\mathrm{mod} h$, 且 $(\beta_1, \cdots, \beta_n, h) = 1$. 则形如 $\alpha_i$ 和 $\alpha_i + \beta_j (1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n)$ 的不同剩余类的个数 $\geqslant \min(m + n, h)$.

**引理 14** 如果 $p > 3$, 则 $N(n, p^\gamma) > 0$.

**证明** 当 $p > 3$ 时, 我们有 $\theta = 0$. 因而, $\gamma = 1$. 同余式 $P(x) \equiv a(\mathrm{mod} p)$ 的解数 $\leqslant 3$. 因此, $P(x)$ 给出至少 $\left[\frac{p}{3}\right] + 1$ 个不同值 $\mathrm{mod} p$. 所以, 由引理 13 知, $P(x_1) + \cdots + P(x_6)$ 给出至少

$$\min\left(p, 5\left[\frac{p}{3}\right] + \left[\frac{p}{3}\right] + 1\right) \geqslant \min\left[p, 6\left(\frac{p}{3} - 1\right) + 1\right] \geqslant p$$

个不同值 $\mathrm{mod} p$. 这就是说, 对于所有的整数 $n$ 和所有的素数 $p$, 同余式

$$P(x_1) + \cdots + P(x_6) \equiv n(\mathrm{mod} p)$$

总可解. 我们可以取 $x_7$, 使得 $p \nmid P^*(x_7)$. 同时, 有整数 $y_1, \cdots, y_6$, 使得

$$P(y_1) + \cdots + P(y_6) \equiv n - P(x_7)(\mathrm{mod} p).$$

因此, 可得引理.

**引理 15** 如果 $p = 3$, 则 $N(n, p^\gamma) > 0$.

**证明** 当 $p = 3$ 时, $\theta = 0$ 或者 1.

(1) 如果 $\theta = 0$, 则 $\gamma = 1$, 引理是平凡的.

(2) 如果 $\theta = 1$, 则 $\gamma = 2$. 如果 $3 \nmid a$, 有 $\theta = 0$. 我们可设 $3|a$. 当 $\theta = 1$ 时, 有 $3|(b, -\frac{1}{6}a + c)$. 因此,

① 可见 Landau. Uber einige Neuere Fortschritte der additiven Zahlentheorie, 第 79 页.

$$P(x)\equiv\frac{a}{3}x^3+d\equiv\frac{a}{3}x+d\ (\mathrm{mod}\ 3).$$

可见 $P(x)$ 给出 0,1 和 2(mod3). 由引理 13 和 $3+5\cdot 2>9$, 可得本引理.

**引理 16**　$N(n,2^\gamma)>0$.

本引理的证明非常复杂, 我们将它分成若干个引理.

我们记

$$\begin{aligned}&P(x)=\frac{a}{2}(x^3-x)+\frac{b}{2}(x^2-x)+cx,\quad 2\nmid(a,b,c),\\&P'(x)=3a\frac{x^2-x}{2}+\left(b+\frac{3a}{2}\right)x-\frac{a}{2}-\frac{b}{2}+c,\\&P''(x)=3ax+b.\end{aligned}$$

这是因为 $\frac{1}{3}$可以被看作整数 mod $2^\gamma$, 而这里的常数项是无关紧要的.

**引理 16.1**　当 $\theta=0$ 时, $P(x)$ 给出至少 $2^{l-2}$ 个不同的奇数且有 $2\nmid P^*(x)$, 或者给出至少 $2^{l-2}$ 个不同的偶数且有 $2\nmid P^*(x)$.

**证明**　因为对于所有的整数 $x$, 有 $P^*(x)\not\equiv 0(\mathrm{mod}\ 2)$, 所以, 当 $l=2$ 时, 引理是显然的. 设 $l\geqslant 3$. 用文 II 的引理 7.6 中的方法, 可得

$$P(x+2^{l+t-1}y)\equiv P(x)+2^{l-1}yP^*(x)(\mathrm{mod}\ 2^l),\tag{1}$$

以及

$$P^*(x)\equiv P^*(y)(\mathrm{mod}\ 2).$$

令 $x_0\equiv x+2^{t+2}$. 则 $P(x_0)$ 和 $P(x_1)$ 给出两个不同的值 mod $2^3$, 它们全为奇数或者全为偶数, 且满足 $2\nmid P^*(x)$. 因此, 对于 $l=3$, 引理成立.

设 $x_1,\cdots,x_{2^{l-3}}$ 为整数, 它们通过 $P(x)$ 给出 $2^{l-3}$ 个不同的值 mod $2^{l-1}$, 且有 $2\nmid P^*(x_i)(i=1,\cdots,2^{l-3})$, 这些值全为奇数或者全为偶数. 因此, 由 (1) 式, 我们取

$$x_1,\cdots,x_{2^{l-3}},x_1+2^{l+t-1},\cdots,x_{2^{l-3}}+2^{l+t-1},$$

这些数满足我们的要求.

**引理 16.2**　当 $\theta=0$ 时, 有 $N(n,2^\gamma)>0$.

**证明**　(1) 如果由引理 16.1 给出的 $2^{l-2}$ 个不同的值都是奇数的话, 由引理 13, 我们可得结果.

(2) 如果由引理 16.1 给出的 $2^{l-2}$ 个不同的值都是偶数的话, 我们用 $P(x)+1$ 代替 $P(x)$, 可得结论.

**引理 16.3**　当 $\theta>0$ 时, 有 $t=0$.

**证明**　假设 $t\neq 0$. 则有 $t=1$ 和

$$\phi'(x)=2P'(x)=3a(x^2-x)+(2b+3a)x+2c-b-a$$

(这里 $\phi'(x)$ 的一个无关紧要的因子 3 可以忽略). 由假设可得 $2|(2b+3a, 2c-b-a)$, 因此, $2|(a,b)$, 但这与 $t \neq 0$ 相矛盾.

今后我们设 $t=0$, 因而, $2|a, 2|b$. 所以, 有 $2 \nmid c$. 不失一般性, 我们可设 $c=1$. 不然的话, 取 $c'$ 为一个整数, 满足 $cc' \equiv 1 (\bmod 2^\gamma)$. 如果对于所有的整数 $n$, 同余式

$$c'P(x_1)+\cdots+c'P(x_7) \equiv n (\bmod 2^\gamma), \quad 2 \nmid P^*(x_1)$$

可解, 这一定有 $N(n, 2^\gamma) > 0$.

其次, 对于 $\theta \geqslant 1$, 我们令

$$2|a, 2|b, 2|\left(3a, b+\frac{3a}{2}, 1-\frac{b}{2}-\frac{a}{2}\right),$$

则有

$$2^2|a \text{ 和 } 2\|b.$$

今后我们记

$$a=2^2a', \quad b=2(2b'+1).$$

**引理 16.4** 当 $\theta=1$ 时, 有 $N(n, 2^\gamma) > 0$.

**证明** 显然, $\gamma \leqslant 4$.

(1) 如果 $2|a', 2|b'$, 则 $P(x)$ 给出 $1, 1+2^3, 0, l_1 (\bmod 2^4)$, 其中 $2^2\|l_1$. 事实上, $P(x) \equiv x^2 (\bmod 2^3)$, 则 $P(0)=0, P(2)=l_1, 2^2\|l_1$; 进一步地, 有 $P(1)=1$ 和 $P(1+2^2) \equiv 1+2^3 (\bmod 2^4)$. 在这种情况里, 引理可以直接验证.

(2) 如果 $2|a', 2 \nmid b'$, 则 $P(x)$ 给出 $0, 2^3, 1, 1+l_2 (\bmod 2^4)$, 其中 $2^2\|l_2$. 证明与 (1) 中相似.

(3) 如果 $2 \nmid a'$, 则 $P(x)$ 给出 $0, 2^3, 1, 1+2^3 (\bmod 2^4)$, 且每一个都满足 $2 \nmid P^*(x)$. 证明也是容易的 (这里要说明的是 7 是最佳可能的).

**引理 16.5** 当 $\theta=2$ 时, 有 $N(n, 2^\gamma) > 0$.

**证明** 此时, $\gamma=5$. 因为 $t=0$ 和 $\theta=2$, 所以, 我们有

$$2|(a,b), 2^2|\left(3a, b+\frac{3a}{2}, 1-\frac{b}{2}-\frac{a}{2}\right).$$

因而

$$a=2^2(2a''+1), \quad b=2(4b''-1).$$

于是, 利用关系式 $x^2-x \equiv 0 (\bmod 2)$, 我们有

$$\begin{aligned} P(2x') &\equiv -2^2x^2+2^3(2-a''+b'')x \ (\bmod 2^5) \\ &\equiv -2^2y^2+2^2(2-a''+b'')^2 \ (\bmod 2^5), \end{aligned}$$

其中

$$y = x - 2 + a'' - b'';$$

还有

$$P(2x+1) \equiv 2^2 \cdot 5x^2 + 3 \cdot 2^3(1+b'')x + 1 \pmod{2^5}.$$

我们可以选取 $\lambda$ 和 $\mu$, 使得

$$h \equiv \lambda + 3 \cdot 2^2(2 - a'' + b'')^2 - 2^2\mu \pmod{2^5},$$
$$0 \leqslant \lambda \leqslant 3, \quad 0 \leqslant \mu < 8.$$

(1) 如果 $\mu \neq 7$, 我们有 $y_1, y_2$ 和 $y_3$, 使得

$$\begin{aligned} n &\equiv \lambda + 3 \cdot 2^2(2 - a'' + b'')^2 - 2^2(y_1^2 + y_2^2 + y_3^2) \pmod{2^5} \\ &\equiv \lambda P(1) + P(x_1) + P(x_2) + P(x_3). \end{aligned}$$

因为 $\lambda \leqslant 3$, 可立得引理.

(2) 如果 $\lambda \neq 3$, 我们有 $y_1, y_2, y_3$ 和 $y_4$, 使得

$$n \equiv \lambda + 4 \cdot 2^2(2 - a'' + b'')^2 - 2^2(y_1^2 + y_2^2 + y_3^2 + y_4^2) \pmod{2^5},$$

因而可得引理.

(3) 假设 $\lambda = 3$ 和 $\mu = 7$.

因为 $P(3) \not\equiv P(1) \pmod{2^5}$, 所以, 我们有

$$n \equiv 2P(1) + P(3) + 3 \cdot 2^2(2 - a'' + b'')^2 - 2^2\mu' \pmod{2^5},$$

和 $\mu' \not\equiv 7 \pmod 8$. 与 §1 中同理, 可得结论.

因为 $\theta \leqslant 2$, 至此我们可以得出引理 16.

**引理 17**　对于所有的 $n$ 和 $P > c_7$, 有 $\mathcal{S}(n) \geqslant c_6 > 0$.

**证明**　我们有

$$|\mathcal{S}(n) - \mathcal{S}'(n)| \leqslant \sum_{q > P^{\frac{8}{9}}} q \cdot q^{-\frac{7}{3}+\varepsilon} = O(P^{-\frac{8}{27}+\varepsilon}).$$

由引理 12,14,15 和 16, 我们有

$$\mathcal{S}(n) \geqslant c_5 > 0.$$

因此

$$\mathcal{S}'(n) \geqslant c_5 + O(P^{-\frac{8}{27}+\varepsilon}) \geqslant c_6.$$

## 5. 定理的证明

**定理** 对于 $N \geqslant c_1$, 我们有 $r_8'(N) > 0$.

**证明** 记

$$T_1(\alpha) = \sum_n e(n\alpha).$$

由引理 4,7 和 11, 我们有

$$\begin{aligned}
r_8'(N) &= \int_0^1 T^7(\alpha) T_1(\alpha) e(-N\alpha) \mathrm{d}\alpha \\
&= \sum_n \int_0^1 T^7(\alpha) e(-(N-n)\alpha) \mathrm{d}\alpha \\
&= \sum_n \sum_{\mathbf{M}_1} q^{*-1} S_{a,q} e\left(-(N-n)\frac{a}{q}\right) \\
&\quad \times \int_{-\infty}^{\infty} I^7(\beta) e(-(N-n)\beta) \mathrm{d}\beta + O(P^{4+\frac{4}{5}-\frac{1}{40}+\varepsilon}) \\
&= \sum_n \mathcal{S}'(N-n) F(N-n) + O(P^{4+\frac{4}{5}-\frac{1}{40}+\varepsilon}) \\
&\geqslant c_7 P^4 \sum_n 1 + O(P^{4+\frac{4}{5}-\frac{1}{40}+\varepsilon}) \\
&\geqslant c_8 P^{4+\frac{4}{5}} + O(P^{4+\frac{4}{5}-\frac{1}{40}+\varepsilon}).
\end{aligned}$$

至此, 定理得证.

(贾朝华 译)

# 关于 Vinogradov 的一个定理[①]

华罗庚 (昆明)

## 1. 引　　言

Vinogradov[②]证明了：如果 $P$ 是一个大的正整数, 则对于满足

$$r < Lk(k+1)(k+2)\log k$$

的最大偶整数 $r$, 有

$$\int_0^1 \cdots \int_0^1 \left|\sum_{x=1}^{P} \mathrm{e}^{2\pi \mathrm{i}(\alpha_k x^k + \cdots + \alpha_1 x)}\right|^r \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k = O(P^{r-\frac{1}{2}k(k+1)}),$$

其中的 $L$(依赖于 $k$) 由下面的表格给出.

| $k$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| $L$ | $4\times 81$ | $4\times 45$ | $4\times 34$ | $4\times 30$ | $4\times 29$ | $4\times 23$ | $4\times 22$ |
| $k$ | 9 | 10 | 11 | 12 | 13 | $\geqslant 14$ | |
| $L$ | $4\times 18$ | $4\times 16$ | $4\times 15$ | $4\times 14$ | $4\times 12$ | $4\times 10$ | |

这个结果很重要, 它有许多的应用. 例如, 在华林问题中的应用, Vinogradov 本人[③]给出的对于三角和估计的应用, 作者[④]给出的在 Tarry 问题和联立华林问题中的应用. 现在, 对于小的 $k$, 我能够改进上述结果. 这就是, 对于下面表格[⑤]所给出的 $s$, 我们有

$$\int_0^1 \cdots \int_0^1 \left|\sum_{x=1}^{P} \mathrm{e}^{2\pi \mathrm{i}(\alpha_k x^k + \cdots + \alpha_1 x)}\right|^s \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k = O(P^{s-\frac{1}{2}k(k+1)+\varepsilon}),$$

这里大 $O$(和以后的等价记号 $\ll$) 常数仅依赖于 $k$ 和 $\varepsilon$.

---

① 1939 年 9 月 26 日收到. 发表于 *Quarterly Journal of Mathematics, Oxford Series*, 1940, 11: 161–176.

② *Recueil Math., new series*, 1938, 3: 435–471.

③ 见脚注②和 *Travaux de l'Institut Math. de Tbilissi*, 1938, 5: 167–180.

④ 参见本文的结尾部分.

⑤ 最后一行是 Vinogradov 给出的值.

| $k$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| $s$ | 6 | 16 | 46 | 124 | 312 | 760 | 1778 | 4068 | 9190 |
| $r$ | 80 | 293 | 721 | 1453 | 2582 | 4148 | 6318 | 9092 | 12644 |

证明方法原则上与我以前文章①中的相似, 但作了更复杂的改进.

我们用 $y\Delta f(x)$ 表示 $f(x+y)-f(x)$. 显然, $\Delta f(x)$ 是 $x$ 和 $y$ 的多项式. $\Delta$ 运算将仅对变量 $x$ 进行. 容易验证

$$y_1\cdots y_\mu\Delta^\mu x^\nu=0\quad(\mu>\nu),$$
$$y_1\cdots y_\mu\Delta^\mu x^\mu=\mu!y_1\cdots y_\mu,$$
$$y_1\cdots y_\mu\Delta^\mu x^{\mu+1}=y_1\cdots y_\mu w,$$

其中 $w$ 是 $y_1,\cdots,y_\mu$ 和 $x$ 的整系数线性型.

**引理 1** 设 $g_1(x),\cdots,g_s(x)$ 为 $x$ 的多项式, 设

$$g(x)=\alpha_1g_1(x)+\cdots+\alpha_sg_s(x)$$

的次数为 $k$. 令

$$F=\sum_{x=1}^{P}\mathrm{e}^{2\pi\mathrm{i}g(x)}.$$

则对于 $\mu=1,2,\cdots,k-1$, 有

$$F^{2^\mu}\ll P^{2^\mu-1}+P^{2^\mu-\mu-1}\sum_{y_1}^{P}\cdots\sum_{y_\mu}^{P}\sum_{x_{\mu+1}}^{P}{}^{*}\mathrm{e}^{2\pi\mathrm{i}y_1\cdots y_\mu\Delta^\mu g(x_{\mu+1})},$$

这里 $\sum_y^P$表示有 $O(P)$ 个项的和式②, 而 $*$ 表示条件 $y_1\cdots y_\mu\Delta^\mu g_r(x_{\mu+1})\neq0$, 其中 $g_r(x)$ 的次数高于 $\mu$.

证明与我以前文章③中的相同.

**定理 $A(k)$** 令

$$f(x)=a_0x^k+a_1x^{k-1}+\cdots,$$

其中 $a_0$ 是一个 $\ll1$ 的整数, 而 $a_1$ 是一个 $\ll P$ 的整数. 令

$$S_k=\sum_{x=1}^{P}\mathrm{e}^{2\pi\mathrm{i}(\alpha_kf(x)+\alpha_{k-2}x^{k-2}+\cdots+\alpha_1x)}.$$

① *Quart. J. Math.* (Oxford), 1938, 9: 199–202.

② 关于 $y_2$ 的求和条件可能依赖于 $y_1$ 的值, 等等.

③ 见脚注①.

则我们有

$$\int_0^1 \cdots \int_0^1 |S_k|^\lambda \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_{k-2}\mathrm{d}\alpha_k = O(P^{\lambda-\frac{1}{2}(k^2-k+2)+\varepsilon}),$$

这里 $\lambda$ 由下面的表格给出.

| $k$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|
| $\lambda$ | 10 | 32 | 86 | 220 | 536 | 1272 | 2930 | 6628 |

**定理 $B(k)$**　令

$$C_k = \sum_{x=1}^{P} \mathrm{e}^{2\pi \mathrm{i}(\alpha_k x^k + \cdots + \alpha_1 x)}.$$

则我们有

$$\int_0^1 \cdots \int_0^1 |C_k|^s \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k = O(P^{s-\frac{1}{2}k(k+1)+\varepsilon}),$$

其中 $s$ 由前面的表格给出.

这两个定理的证明相互依赖. 准确地讲, 我将用 $A(l_1)$ 和 $B(l_2)(l_1 \leqslant k-1, l_2 \leqslant k-1)$ 证明中的结果来证明定理 $A(k)$, 并且用 $A(l_1)$ 和 $B(l_2)(l_1 \leqslant k-1, l_2 \leqslant k-1)$ 证明中的结果来证明定理 $B(k)$. 对于不同的 $k$ 值, 所用的方法也不同. 当然, 对于归纳法可以有一个统一的方法, 但那样得到的结果比较差.

## 2. 定理的证明

2.01. 我们只要在表述上作一点小的改动, 就可以在 $A(k)$ 中假设 $f(x) = x^k$. 事实上,

$$\int_0^1 \cdots \int_0^1 |S_k|^{2\mu} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_{k-2}\mathrm{d}\alpha_k$$

等于方程组

$$f(x_1) + \cdots + f(x_\mu) = f(y_1) + \cdots + f(y_\mu),$$
$$x_1^{k-2} + \cdots + x_\mu^{k-2} = y_1^{k-2} + \cdots + y_\mu^{k-2},$$
$$\cdots\cdots$$
$$x_1 + \cdots + x_\mu = y_1 + \cdots + y_\mu$$

的解数, 这里的限制条件为

$$1 \leqslant x_\nu \leqslant P, \quad 1 \leqslant y_\nu \leqslant P \quad (\nu = 1, 2, \cdots, \mu).$$

将以上的等式分别乘以 $k^k a_0^{k-1}, k^{k-2}a_0^{k-2}, \cdots, ka_0$, 可得

$$\sum_{\nu=1}^{\mu}((ka_0x_\nu)^k + ka_1(ka_0x_\nu)^{k-1} + \cdots)$$

$$= \sum_{\nu=1}^{\mu}((ka_0y_\nu)^k + ka_1(ka_0y_\nu)^{k-1} + \cdots),$$

$$\sum_{\nu=1}^{\mu}(ka_0x_\nu)^{k-2} = \sum_{\nu=1}^{\mu}(ka_0y_\nu)^{k-2},$$

$$\cdots\cdots$$

$$\sum_{\nu=1}^{\mu}(ka_0x_\nu) = \sum_{\nu=1}^{\mu}(ka_0y_\nu).$$

记

$$x'_\nu = ka_0x_\nu + a_1, y'_\nu = ka_0y_\nu + a_1.$$

则我们有方程组

$$\begin{cases} x_1'^k + \cdots + x_\mu'^k = y_1'^k + \cdots + y_\mu'^k, \\ x_1'^{k-2} + \cdots + x_\mu'^{k-2} = y_1'^{k-2} + \cdots + y_\mu'^{k-2}, \\ \qquad\cdots\cdots \\ x'_1 + \cdots + x'_\mu = y'_1 + \cdots + y'_\mu, \end{cases} \tag{1}$$

限制条件为

$$a_0k|(x'_\nu - a_1), \tag{2}$$

$$a_1 + 1 \leqslant x'_\nu \leqslant a_1 + P. \tag{3}$$

于是

$$\int_0^1 \cdots \int_0^1 |S_k|^{2\mu} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_{k-2} \mathrm{d}\alpha_k$$

肯定不超过方程组 (1) 在限制条件 (3) 之下的解数. 因此, 只要假定在定理 $A(k)$ 和 $B(k)$ 中, 我们允许求和范围在任一个长度为 $P$ 且两个端点均 $\ll P$ 的区间里, 那么, 我们只需讨论特殊情形 $f(x) = x^k$ 就可以了. 从现在起, 我们就采用这种稍微一般的假定.

2.02. 我们现在来证明

$$\int_0^1 \cdots \int_0^1 |S_k|^{2k} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \ll P^{k+\varepsilon}. \tag{4}$$

为此, 我们需要下面的

**引理 2** 设

$$s_i = x_1^i + \cdots + x_k^i \quad (i = 1, 2, \cdots, k).$$

则 $x_1, \cdots, x_k$ 的对称函数

$$f = (s_1 - x_1) \cdots (s_1 - x_k)$$

可以表作 $s_1, \cdots, s_{k-2}$ 和 $s_k$ 的一个函数.

**证明** 我们记

$$f = s_1^k - s_1^{k-1}\sigma_1 + \cdots + (-1)^k \sigma_k,$$

这里 $\sigma_i$ 为 $x_1, \cdots, x_k$ 的第 $i$ 个初等对称函数. 由对称函数的一个熟知结果, 我们有

$$f = (-1)^k \sigma_k + (-1)^{k-1} \sigma_{k-1} s_1 + f_1(s_1, \cdots, s_{k-2}). \tag{5}$$

由牛顿公式, 可得

$$(-1)^k k \sigma_k = -s_k + \sigma_1 s_{k-1} + (-1)^k \sigma_{k-1} s_1 + f_2(s_1, \cdots, s_{k-2})$$

和

$$(-1)^{k-1}(k-1)\sigma_{k-1} = -s_{k-1} + f_3(s_1, \cdots, s_{k-2}).$$

从而有

$$\begin{aligned} & k((-1)^k \sigma_k + (-1)^{k-1} \sigma_{k-1} s_1) \\ = & -s_k + \sigma_1 s_{k-1} - s_1 s_{k-1} + f_4(s_1, \cdots, s_{k-2}) \\ = & -s_k + f_4(s_1, \cdots, s_{k-2}). \end{aligned}$$

由此及 (5) 式, 我们可得引理.

2.03. (4) 式的证明. (4) 式左端的积分不超过方程组

$$\begin{cases} x_1^k + \cdots + x_k^k = y_1^k + \cdots + y_k^k, \\ x_1^{k-2} + \cdots + x_k^{k-2} = y_1^{k-2} + \cdots + y_k^{k-2}, \\ \qquad \cdots\cdots \\ x_1 + \cdots + x_k = y_1 + \cdots + y_k \end{cases} \tag{6}$$

的解数, 这里的限制条件为

$$x_\nu = O(P), \quad y_\nu = O(P).$$

令

$$l = x_1 + \cdots + x_k = y_1 + \cdots + y_k.$$

由引理 2 知, 方程组 (6) 可推出

$$(l - x_1) \cdots (l - x_k) = (l - y_1) \cdots (l - y_k).$$

对于给定的 $y_1, \cdots, y_k$, 如果它们满足条件

$$(l - y_1) \cdots (l - y_k) \neq 0, \tag{7}$$

则 $x_1, \cdots, x_k$ 的组数不超过

$$d^k((l-y_1)\cdots(l-y_k)) = O(P^\varepsilon),$$

这里 $d(n)$ 表示 $n$ 的因子的个数.

如果 (7) 式不成立, 则有一个 $y$ 和一个 $x$ 等于 $l$. 设 $x_k = y_k = l$. 对于 $x_k$, 有 $O(P)$ 种选择. (6) 式可以推出

$$x_1^{k-2} + \cdots + x_{k-1}^{k-2} = y_1^{k-2} + \cdots + y_{k-1}^{k-2},$$
$$\cdots\cdots$$
$$x_1 + \cdots + x_{k-1} = y_1 + \cdots + y_{k-1} = 0.$$

对于 $x_{k-1}, y_2, \cdots, y_{k-1}$, 有 $O(P^{k-1})$ 种选择. 对于其中的每一种选择, 可以唯一地确定 $y_1$, 而对应的 $x_1, \cdots, x_{k-2}$ 不超过 $(k-2)!(= O(1))$ 种可能. 因此, 在这种情形里, (6) 式的解数为 $O(P^{k+\varepsilon})$. 由此证明了 (4) 式.

2.04. 接下来, 我们将证明

$$\int_0^1 \cdots \int_0^1 |C_k|^{2(k+1)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \ll P^{k+1+\varepsilon}. \tag{8}$$

为此, 我们需要下面的

**引理 3** 由方程组

$$x_1^k + \cdots + x_{k+1}^k = y_1^k + \cdots + y_{k+1}^k,$$
$$x_1^{k-1} + \cdots + x_{k+1}^{k-1} = y_1^{k-1} + \cdots + y_{k+1}^{k-1},$$
$$\cdots\cdots$$
$$x_1 + \cdots + x_{k+1} = y_1 + \cdots + y_{k+1}, \tag{9}$$

可以导出一个形如

$$\begin{aligned}&(x_{k+1} - y_{k+1}) g(y_1, \cdots, y_k, x_k, y_{k+1}, x_{k+1})\\ =\ &(x_k - y_k) h(y_1, \cdots, y_k, x_k)\end{aligned}$$

的关系式, 其中 $g$ 和 $h$ 为其变量的 $k-1$ 次齐次多项式. 包含在 $g$ 中的只含 $x_{k+1}$ 和 $y_{k+1}$ 的 $k-1$ 次齐次多项式不能被 $x_{k+1} - y_{k+1}$ 整除. $h$ 中 $x_k^{k-1}$ 项的系数和 $g$ 中 $x_{k+1}^{k-1}$ 项的系数均为非零常数.

**证明** 设

$$s_i = x_1^i + \cdots + x_{k-1}^i, \quad t_i = y_1^i + \cdots + y_{k-1}^i.$$

我们可以将 (9) 式写成

$$s_\nu = t_\nu - (x_k^\nu - y_k^\nu) - (x_{k+1}^\nu - y_{k+1}^\nu) \quad (\nu = 1, \cdots, k). \tag{10}$$

众所周知

$$s_k - \sigma_1 s_{k-1} + \sigma_2 s_{k-2} + \cdots + (-1)^{k-1}\sigma_{k-1}s_1 = 0, \tag{11}$$

其中 $\sigma_i$ 为 $x_1, \cdots, x_{k-1}$ 的第 $i$ 个初等对称函数. 因为 $\sigma_i$ 可以表作 $s_1, \cdots, s_i$ 的一个多项式, 所以, 我们可以将 (11) 式记作

$$s_k - s_1 s_{k-1} + \sigma_2(s_1, s_2)s_{k-2} + \cdots + (-1)^{k-1}\sigma_{k-1}(s_1, \cdots, s_{k-1})s_1 = 0. \tag{12}$$

类似地, 有

$$t_k - t_1 t_{k-1} + \sigma_2(t_1, t_2)t_{k-2} + \cdots + (-1)^{k-1}\sigma_{k-1}(t_1, \cdots, t_{k-1})t_1 = 0. \tag{13}$$

如果将 (10) 式代到 (12) 式中去, 我们可以得到 (13) 式的左端加上若干项, 其中每一项均为 $t$ 的方幂与形如 $x_k^\nu - y_k^\nu, x_{k+1}^\nu - y_{k+1}^\nu$ 的因子之积. 我们减去 (13) 式, 并将所有不含 $x_{k+1}^\nu - y_{k+1}^\nu$ 因子的项移到右边去, 就可以得到所需要的关系式.

$g$ 中只含 $x_{k+1}$ 和 $y_{k+1}$ 的部分来自那些仅含 $x_{k+1}^\nu - y_{k+1}^\nu$ 因子的项. 在其中除去来自 $s_k$ 的 $-(x_{k+1}^k - y_{k+1}^k)$ 项外, 其余的均含至少两个因子. 这个例外项不能被 $(x_{k+1} - y_{k+1})^2$ 整除, 而其他项可以. 这就证明了关于 $g$ 的结论.

在用 (10) 式代入 (12) 式所得到的表达式中, 可以通过令 $s_\nu = -x_{k+1}^\nu$ 来得到 $x_{k+1}^k$ 项的系数. 这样, 就有 $\sigma_\nu = (-1)^\nu x_{k+1}^\nu$, 而系数为

$$-1 - (-1)(-1) + (1)(-1) - \cdots + (-1)^{k-1}(-1)^{k-1}(-1) = -k. \tag{14}$$

因此, $g$ 中 $x_{k+1}^{k-1}$ 项的系数为 $-k$. 对于 $h$ 中 $x_k^{k-1}$ 项的系数也有相似的结论.

2.05. (8) 式的证明. 左端的积分为方程组 (9) 在限制条件 $x_\nu = O(P), y_\nu = O(P)$ 下的解数. 由引理 3, 方程组可以导出关系式

$$(x_{k+1} - y_{k+1})g(y_1, \cdots, y_k, x_k, y_{k+1}, x_{k+1}) = (x_k - y_k)h(y_1, \cdots, y_k, x_k). \tag{15}$$

对于给定的 $y_1, \cdots, y_k, x_k$, 如果它们满足

$$(x_k - y_k)h(y_1, \cdots, y_k, x_k) \neq 0, \tag{16}$$

则 $x_{k+1}, y_{k+1}$ 的组数为

$$O(d\{(x_k - y_k)h(y_1, \cdots, y_k, x_k)\}) = O(P^\varepsilon).$$

事实上, 由引理 3 的第二个结论, 满足

$$x_{k+1}-y_{k+1}=c, g(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})=d$$

($c,d$ 为非零整数) 的 $x_{k+1},y_{k+1}$ 的组数不超过 $g$ 的次数 $k-1$.

进一步地, 如果

$$(x_k-y_k)h(y_1,\cdots,y_k,x_k)=0,$$

则

$$(x_{k+1}-y_{k+1})g(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})=0.$$

由引理 3 的最后一个结论知, 对于给定的 $y_1,\cdots,y_k,y_{k+1}$, 这两个方程可以推出, 仅有 $O(1)$ 个可能的 $x_k$ 和 $x_{k+1}$.

在两种情形里, 当 $y_1,\cdots,y_k,x_k,x_{k+1},y_{k+1}$ 已知, 由 (9) 式可得, 仅有 $O(1)$ 组可能的 $x_1,\cdots,x_{k-1}$. 因此, 方程组 (9) 在限制条件 $x_\nu=O(P),y_\nu=O(P)$ 下的解数为 $O(P^{k+1+\varepsilon})$. 这就证明了 (8) 式.

2.06. $B(2)$ 为 (8) 式当 $k=2$ 时的特殊情形.

2.07. $A(3)$ 的证明. 由引理 1 可得

$$|S_3|^4\ll P^3+P\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{x_3}^{P}{}^{*}\mathrm{e}^{2\pi\mathrm{i}y_1y_2\Delta^2(\alpha_3x_3^3+\alpha_1x_3)},$$

这里 $*$ 表示变量满足条件 $y_1y_2\Delta^2x_3^3\neq0$. 将此不等式乘以 $|S_3|^6$, 并对于 $\alpha_1$ 和 $\alpha_3$ 积分, 可得

$$\int_0^1\int_0^1|S_3|^{10}\mathrm{d}\alpha_1\mathrm{d}\alpha_3\ll P^3\int_0^1\int_0^1|S_3|^6\mathrm{d}\alpha_1\mathrm{d}\alpha_3+PR,$$

这里 $R$ 表示方程组

$$y_1y_2\Delta^2(x_3^3)=z_1^3+\cdots+z_3^3-z_4^3-\cdots-z_6^3\quad(y_1y_2\Delta^2(x_3^3)\neq0),$$
$$0=z_1+\cdots+z_3-z_4-\cdots-z_6$$

的解数, 其中 $z_\nu=O(P)$. 因为给定 $z_1,\cdots,z_5$ 之后, 其他的变量只有 $O(P^\varepsilon)$ 种可能, 所以, 我们有 $R=O(P^{5+\varepsilon})$. 因此, 应用 (4) 式 (取 $k=3$), 我们有

$$\int_0^1\int_0^1|S_3|^{10}\mathrm{d}\alpha_1\mathrm{d}\alpha_3\ll P^{6+\varepsilon}.\tag{17}$$

2.08. $B(3)$ 的证明. 由引理 1 可得

$$|C_3|^4\ll P^3+P\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{x_3}^{P}{}^{*}\mathrm{e}^{2\pi\mathrm{i}y_1y_2\Delta^2(\alpha_3x_3^3+\alpha_2x_3^2)},\tag{18}$$

这里 $*$ 表示变量满足条件

$$y_1y_2\Delta^2(x_3^3)\neq 0,\quad y_1y_2\Delta^2(x_3^2)\neq 0.$$

将此不等式乘以 $|C_3|^8$, 对于 $\alpha_1,\alpha_2,\alpha_3$ 积分, 并用 (8) 式 ($k=3$), 可得

$$\int_0^1\int_0^1\int_0^1|C_3|^{12}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_3\ll P^{7+\varepsilon}+PR,$$

这里 $R$ 表示方程组

$$\begin{aligned}y_1y_2w&=z_1^3+\cdots+z_4^3-z_5^3-\cdots-z_8^3(y_1y_2w\neq 0),\\2y_1y_2&=z_1^2+\cdots+z_4^2-z_5^2-\cdots-z_8^2,\\0&=z_1+\cdots+z_4-z_5-\cdots-z_8\end{aligned}$$

的解数, 其中 $w=\Delta^2(x_3^3)\ll P, z_\nu\ll P$.

对于任意固定的 $w$, 由 (4) 式 ($k=3$) 和 $f(z)=2z^3-wz^2$ 知, 方程组

$$\begin{aligned}&(2z_1^3-wz_1^2)+\cdots+(2z_4^3-wz_4^2)\\&=(2z_5^3-wz_5^2)+\cdots+(2z_8^3-wz_8^2),\\&z_1+\cdots+z_4=z_5+\cdots+z_8\end{aligned}$$

的解数为 $O(P^{5+\varepsilon})$. 因此, $R=O(P^{6+\varepsilon})$, 从而,

$$\int_0^1\int_0^1\int_0^1|C_3|^{12}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_3\ll P^{7+\varepsilon}.\tag{19}$$

同理, 将 (18) 式乘以 $|C_3|^{12}$, 应用 (19) 式和

$$\int_0^1\int_0^1|S_3|^{12}\mathrm{d}\alpha_1\mathrm{d}\alpha_3\ll P^{8+\varepsilon}$$

(这是 (17) 式的平凡推论), 我们可得

$$\int_0^1\int_0^1\int_0^1|C_3|^{16}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_3\ll P^{10+\varepsilon},$$

即为 $B(3)$.

2.09.$A(4)$ 的证明. 由引理 1 可得

$$|S_4|^8\ll P^7+P^4\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{y_3}^{P}\sum_{x_4}^{P}{}^{*}\mathrm{e}^{2\pi\mathrm{i}y_1y_2y_3\Delta^3(\alpha_4x_4^4+\alpha_2x_4^2+\alpha_1x_4)},$$

这里 $*$ 表示 $y_1y_2y_3\Delta^3x_4^4\neq 0$. 乘以 $|S_4|^8$ 后积分, 并用 (4) 式 ($k=4$), 我们有

$$\int_0^1\int_0^1\int_0^1|S_4|^{16}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_4\ll P^{11+\varepsilon}+P^4R,$$

这里 $R$ 表示方程组

$$\begin{aligned}y_1y_2y_3\Delta^3x_4^4 &= z_1^4+\cdots+z_4^4-z_5^4-\cdots-z_8^4 \quad (y_1y_2y_3\Delta^3x_4^4\neq 0),\\ 0&=z_1^2+\cdots+z_4^2-z_5^2-\cdots-z_8^2,\\ 0&=z_1+\cdots+z_4-z_5-\cdots-z_8\end{aligned}$$

的解数, 其中 $z_\nu \ll P$. 用

$$\int_0^1\int_0^1 |C_2|^8\mathrm{d}\alpha_1\mathrm{d}\alpha_2 \ll P^{5+\varepsilon}$$

(这是 $B(2)$ 的平凡推论), 我们有 $R\ll P^{5+\varepsilon}$. 因此,

$$\int_0^1\int_0^1\int_0^1 |S_4|^{16}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_4 \ll P^{11+\varepsilon}. \tag{20}$$

重复同样的讨论, 分别乘以 $|S_4|^{16}$ 和 $|S_4|^{24}$, 我们可得

$$\int_0^1\int_0^1\int_0^1 |S_4|^{24}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_4 \ll P^{18+\varepsilon} \tag{21}$$

和

$$\int_0^1\int_0^1\int_0^1 |S_4|^{32}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_4 \ll P^{25+\varepsilon}. \tag{22}$$

即为 $A(4)$.

2.10. $B(4)$ 的证明. 由引理 1 可得

$$|C_4|^4 \ll P^3 + P\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{x_3}^{P}{}^{*}\mathrm{e}^{2\pi\mathrm{i}y_1y_2\Delta^2(\alpha_4x_3^4+\alpha_3x_3^3+\cdots)},$$

这里 $*$ 表示变量满足条件

$$y_1y_2\Delta^2x_3^4\neq 0, \quad y_1y_2\Delta^2x_3^3\neq 0.$$

将此不等式乘以 $|C_4|^{10}$ 并积分, 应用 (8) 式, 我们有

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{14}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_3\mathrm{d}\alpha_4 \ll P^{8+\varepsilon}+PR,$$

这里 $R$ 表示方程组

$$\begin{aligned}y_1y_2\Delta^2x_3^4 &= z_1^4+\cdots-z_{10}^4 \quad (y_1y_2\Delta^2x_3^4\neq 0),\\ y_1y_2w &= z_1^3+\cdots-z_{10}^3 \quad (y_1y_2w\neq 0),\\ 2y_1y_2 &= z_1^2+\cdots-z_{10}^2,\\ 0&=z_1+\cdots-z_{10}\end{aligned}$$

的解数 (关于 $w$ 和 $z_i$ 大小的通常条件是不言自明的). 对于固定的 $w$, 由 (17) 式知, 方程组

$$0 = (2z_1^3 - wz_1^2) + \cdots - (2z_{10}^3 - wz_{10}^2),$$
$$0 = z_1 + \cdots - z_{10}$$

的解数为 $O(P^{6+\varepsilon})$. 因此, $R = O(P^{7+\varepsilon})$, 从而,

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{14}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_3\mathrm{d}\alpha_4 \ll P^{8+\varepsilon}. \tag{23}$$

由引理 1 可得

$$|C_4|^8 \ll P^7 + P^4\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{y_3}^{P}\sum_{x_4}^{P}{}^{*}\mathrm{e}^{2\pi i y_1y_2y_3\Delta^3(\alpha_4x_4^4+\cdots)},$$

这里 $*$ 表示 $y_1y_2y_3\Delta^3x_4^4 \neq 0$. 乘以 $|C_4|^{14}$ 并积分, 应用 (23) 式, 我们有

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{22}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_4 \ll P^{15+\varepsilon} + P^4R,$$

这里 $R$ 表示方程组

$$y_1y_2y_3w = z_1^4 + \cdots - z_{14}^4 \quad (y_1y_2y_3w \neq 0),$$
$$6y_1y_2y_3 = z_1^3 + \cdots - z_{14}^3,$$
$$0 = z_1^2 + \cdots - z_{14}^2,$$
$$0 = z_1 + \cdots - z_{14}$$

的解数. 显然, 对于固定的 $w, R$ 不超过方程组

$$(6z_1^4 - wz_1^3) + \cdots - (6z_{14}^4 - wz_{14}^3) = 0,$$
$$z_1^2 + \cdots - z_{14}^2 = 0,$$
$$z_1 + \cdots - z_{14} = 0$$

解数的 $P^{1+\varepsilon}$ 倍. 由 (4) 式的一个平凡推论, 我们有

$$\int_0^1\int_0^1\int_0^1 |S_4|^{14}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_4 \ll P^{10+\varepsilon}.$$

因而, $R \ll P^{11+\varepsilon}$. 由此可得

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{22}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_4 \ll P^{15+\varepsilon}. \tag{24}$$

用相同的方法, 并分别用 (20),(21),(22) 式代替 (4) 式, 我们可得

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{30}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_4 \ll P^{22+\varepsilon}, \tag{25}$$

$$\int_0^1 \int_0^1 \int_0^1 \int_0^1 |C_4|^{38} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_4 \ll P^{29+\varepsilon}, \tag{26}$$

$$\int_0^1 \int_0^1 \int_0^1 \int_0^1 |C_4|^{46} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_4 \ll P^{36+\varepsilon}. \tag{27}$$

最后一个即为 $B(4)$.

从现在起, 我们将用缩写

$$\int f \mathrm{d}\alpha$$

代替

$$\int_0^1 \cdots \int_0^1 f(\alpha_1, \cdots, \alpha_n) \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_n.$$

2.11. $A(5)$ 的证明. 由引理 1 可得,

$$|S_5|^4 \ll P^3 + P \sum_{y_1}^{P} \sum_{y_2}^{P} \sum_{x_3}^{P}{}^{*} \mathrm{e}^{2\pi \mathrm{i} y_1 y_2 \Delta^2 g(x_3)},$$

这里

$$g(x) = \alpha_5 x^5 + \alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x.$$

乘以 $|S_5|^{10}$ 并积分, 由 (4) 式, 我们有

$$\int |S_5|^{14} \mathrm{d}\alpha \ll P^{8+\varepsilon} + PR,$$

这里 $R$ 表示方程组

$$\begin{aligned} y_1 y_2 \Delta^2 x_3^5 &= z_1^5 + \cdots - z_{10}^5 \quad (y_1 y_2 \Delta^2 x_3^5 \neq 0), \\ y_1 y_2 w &= z_1^3 + \cdots - z_{10}^3 \quad (y_1 y_2 w \neq 0), \\ 2 y_1 y_2 &= z_1^2 + \cdots - z_{10}^2, \\ 0 &= z_1 + \cdots - z_{10} \end{aligned}$$

的解数. 对于固定的 $w$, 由 $A(3)$, 方程组

$$\begin{aligned} (2z_1^3 - w z_1^2) + \cdots - (2z_{10}^3 - w z_{10}^2) &= 0, \\ z_1 + \cdots - z_{10} &= 0 \end{aligned}$$

的组数 $\ll P^{6+\varepsilon}$. 因此, $R \ll P^{7+\varepsilon}$, 从而

$$\int |S_5|^{14} \mathrm{d}\alpha \ll P^{8+\varepsilon}. \tag{28}$$

由引理 1 可得

$$|S_5|^8 \ll P^7 + P^4 \sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{y_3}^{P}\sum_{x_4}^{P}{}^{*} \mathrm{e}^{2\pi \mathrm{i} y_1 y_2 y_3 \Delta^3 g(x_4)}.$$

乘以 $|S_5|^{14}$ 并积分, 由 (28) 式, 我们有

$$\int |S_5|^{22}\mathrm{d}\alpha \ll P^{15+\varepsilon} + P^4 R,$$

这里 $R$ 表示方程组

$$\begin{aligned} y_1y_2y_3\Delta^3 x_3^5 &= z_1^5 + \cdots - z_{14}^5 \quad (y_1y_2y_3\Delta^3x_3^5 \neq 0), \\ 6y_1y_2y_3 &= z_1^3 + \cdots - z_{14}^3, \\ 0 &= z_1^2 + \cdots - z_{14}^2, \\ 0 &= z_1 + \cdots - z_{14} \end{aligned}$$

的解数. 显然, 由 $B(2)$ 的一个平凡推论, 有

$$R \ll P^{\varepsilon} \int |C_2|^{14}\mathrm{d}\alpha \ll P^{11+\varepsilon}.$$

因此

$$\int |S_5|^{22}\mathrm{d}\alpha \ll P^{15+\varepsilon}. \tag{29}$$

由引理 1 可得

$$|S_5|^{16} \ll P^{15} + P^{11} \sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{y_3}^{P}\sum_{y_4}^{P}\sum_{x_5}^{P}{}^{*} \mathrm{e}^{2\pi \mathrm{i} y_1 y_2 y_3 y_4 \Delta^4 g(x_5)}.$$

乘以 $|S_5|^{22}$ 并积分, 我们可得

$$\int |S_5|^{38}\mathrm{d}\alpha \ll P^{30+\varepsilon} + P^{11} R.$$

由 $B(3)$ 的一个平凡推论, 易见

$$R \ll P^{\varepsilon} \int |C_3|^{22}\mathrm{d}\alpha \ll P^{16+\varepsilon}.$$

因而

$$\int |S_5|^{38}\mathrm{d}\alpha \ll P^{30+\varepsilon}.$$

反复这个过程, 我们可得

$$\int |S_5|^{38+16\lambda}\mathrm{d}\alpha \ll P^{30+15\lambda+\varepsilon} \quad (\lambda = 0, 1, 2, 3). \tag{30}$$

当 $\lambda = 3$ 时, 即为 $A(5)$.

2.12. $B(5)$ 的证明. 由引理 1 可得

$$|C_5|^8 \ll P^7 + P^4 \sum_{y_1}^{P} \sum_{y_2}^{P} \sum_{y_3}^{P} \sum_{x_4}^{P}{}^{*} e^{2\pi i y_1 y_2 y_3 \Delta^3(\alpha_5 x_4^5 + \alpha_4 x_4^4 + \cdots)}.$$

将此不等式乘以 $|C_5|^{12}$ 并积分, 应用 (8) 式, 我们有

$$\int |C_5|^{20} \mathrm{d}\alpha \ll P^{13+\varepsilon} + P^4 R.$$

由 (4) 式的一个平凡推论, 易见

$$R \ll P^{1+\varepsilon} \int |S_4|^{12} \mathrm{d}\alpha \ll P^{9+\varepsilon}.$$

因而

$$\int |C_5|^{20} \mathrm{d}\alpha \ll P^{13+\varepsilon}.$$

重复这种讨论, 并分别用 (20),(21),(22) 式代替 (4) 式, 我们可得

$$\int |C_5|^{20+8\lambda} \mathrm{d}\alpha \ll P^{13+7\lambda+\varepsilon} \quad (\lambda = 1, 2, 3). \tag{31}$$

用引理 $1(\mu = 4)$ 和 (30) 式, 可得

$$\int |C_5|^{44+16\lambda} \mathrm{d}\alpha \ll P^{34+15\lambda+\varepsilon} \quad (\lambda = 1, 2, 3, 4, 5). \tag{32}$$

当 $\lambda = 5$ 时, 即为 $B(5)$.

2.13. $A(6)$ 的证明. 由引理 $1(\mu = 3)$ 和 $A(4)$ 证明中的结果, 我们可得

$$\int |S_6|^{12+8\lambda} \mathrm{d}\alpha \ll P^{6+7\lambda+\varepsilon} \quad (\lambda = 1, 2, 3, 4). \tag{33}$$

由引理 $1(\mu = 4)$ 和 $B(3)$, 我们可得

$$\int |S_6|^{60} \mathrm{d}\alpha \ll P^{49+\varepsilon}. \tag{34}$$

由引理 $1(\mu = 5)$ 和 $B(4)$ 证明中的结果, 我们可得

$$\int |S_6|^{60+32\lambda} \mathrm{d}\alpha \ll P^{49+31\lambda+\varepsilon} \quad (\lambda = 1, 2, 3, 4, 5). \tag{35}$$

当 $\lambda = 5$ 时, 即为 $A(6)$.

2.14. $B(6)$ 的证明. 这里, 我们将从 (8) 式开始的地方代之以从

$$\int |C_6|^{16}\mathrm{d}\alpha \ll P^{9+\varepsilon}$$

(这是 (8) 式的一个显然推论) 开始. 由引理 $1(\mu=3)$ 和 $A(4)$ 证明中的结果, 我们可得

$$\int |C_6|^{16+8\lambda}\mathrm{d}\alpha \ll P^{9+7\lambda+\varepsilon} \quad (\lambda=1,2,3). \tag{36}$$

由引理 $1(\mu=4)$ 和 $A(5)$ 证明中的结果, 可得

$$\int |C_6|^{40+16\lambda}\mathrm{d}\alpha \ll P^{30+15\lambda+\varepsilon} \quad (\lambda=1,2,3,4,5). \tag{37}$$

由引理 $1(\mu=5)$ 和 $A(6)$ 证明中的结果, 可得

$$\int |C_6|^{120+32\lambda}\mathrm{d}\alpha \ll P^{105+31\lambda+\varepsilon} \quad (\lambda=1,2,3,4,5,6). \tag{38}$$

2.15. $A(7)$ 的证明. 作为 (4) 式的一个显然推论, 我们有

$$\int |S_7|^{16}\mathrm{d}\alpha \ll P^{9+\varepsilon}.$$

由引理 $1(\mu=3)$ 和 $A(4)$ 证明中的结果, 我们有

$$\int |S_7|^{16+8\lambda}\mathrm{d}\alpha \ll P^{9+7\lambda+\varepsilon} \quad (\lambda=1,2,3). \tag{39}$$

由引理 $1(\mu=4)$ 和 $A(5)$ 证明中的结果, 可得

$$\int |S_7|^{40+16\lambda}\mathrm{d}\alpha \ll P^{30+15\lambda+\varepsilon} \quad (\lambda=1,2,3,4,5). \tag{40}$$

由引理 $1(\mu=5)$ 和 (27) 式, 可得

$$\int |S_7|^{152}\mathrm{d}\alpha \ll P^{136+\varepsilon}. \tag{41}$$

由引理 $1(\mu=6)$ 和 $B(5)$ 证明中的结果, 可得

$$\int |S_7|^{152+64\lambda}\mathrm{d}\alpha \ll P^{136+63\lambda+\varepsilon} \quad (\lambda=1,2,3,4,5,6). \tag{42}$$

2.16. $B(7)$ 的证明. 作为 (8) 式的一个显然推论, 我们有

$$\int |C_7|^{24}\mathrm{d}\alpha \ll P^{16+\varepsilon}.$$

与 $A(7)$ 的证明一样, 我们可得

$$\int |C_7|^{24+8\lambda}\mathrm{d}\alpha \ll P^{16+7\lambda+\varepsilon} \quad (\lambda = 1, 2), \tag{43}$$

$$\int |C_7|^{40+16\lambda}\mathrm{d}\alpha \ll P^{30+15\lambda+\varepsilon} \quad (\lambda = 1, 2, 3, 4, 5), \tag{44}$$

$$\int |C_7|^{120+32\lambda}\mathrm{d}\alpha \ll P^{105+31\lambda+\varepsilon} \quad (\lambda = 1, 2, 3, 4, 5, 6), \tag{45}$$

$$\int |C_7|^{312+64\lambda}\mathrm{d}\alpha \ll P^{291+63\lambda+\varepsilon} \quad (\lambda = 1, 2, 3, 4, 5, 6, 7). \tag{46}$$

2.17. $A(8)$ 的证明. 作为 (4) 式的一个显然推论, 我们有

$$\int |S_8|^{24}\mathrm{d}\alpha \ll P^{16+\varepsilon}.$$

此外, 我们还有

$$\int |S_8|^{24+8\lambda}\mathrm{d}\alpha \ll P^{16+7\lambda+\varepsilon} \quad (\lambda = 1, 2), \tag{47}$$

$$\int |S_8|^{40+16\lambda}\mathrm{d}\alpha \ll P^{30+15\lambda+\varepsilon} \quad (\lambda = 1, 2, 3, 4, 5), \tag{48}$$

$$\int |S_8|^{120+32\lambda}\mathrm{d}\alpha \ll P^{105+31\lambda+\varepsilon} \quad (\lambda = 1, 2, 3, 4, 5, 6), \tag{49}$$

$$\int |S_8|^{376}\mathrm{d}\alpha \ll P^{354+\varepsilon}, \tag{50}$$

$$\int |S_8|^{376+128\lambda}\mathrm{d}\alpha \ll P^{354+127\lambda+\varepsilon} \quad (\lambda = 1, 2, \cdots, 7). \tag{51}$$

2.18. $B(8)$ 的证明. 我们有

$$\int |C_8|^{18+16\lambda}\mathrm{d}\alpha \ll P^{9+15\lambda+\varepsilon} \quad (\lambda = 1, 2, 3, 4, 5, 6), \tag{52}$$

$$\int |C_8|^{114+32\lambda}\mathrm{d}\alpha \ll P^{99+31\lambda+\varepsilon} \quad (\lambda = 1, 2, 3, 4, 5, 6), \tag{53}$$

$$\int |C_8|^{306+64\lambda}\mathrm{d}\alpha \ll P^{285+63\lambda+\varepsilon} \quad (\lambda = 1, 2, \cdots, 7), \tag{54}$$

$$\int |C_8|^{754+128\lambda}\mathrm{d}\alpha \ll P^{726+127\lambda+\varepsilon} \quad (\lambda = 1, 2, \cdots, 8). \tag{55}$$

2.19. $A(9)$ 的证明. 我们有

$$\int |S_9|^{18+16\lambda}\mathrm{d}\alpha \ll P^{9+15\lambda+\varepsilon} \quad (\lambda = 1, 2, 3, 4, 5, 6), \tag{56}$$

$$\int |S_9|^{114+32\lambda}\mathrm{d}\alpha \ll P^{99+31\lambda+\varepsilon} \quad (\lambda=1,2,3,4,5,6), \tag{57}$$

$$\int |S_9|^{306+64\lambda}\mathrm{d}\alpha \ll P^{285+63\lambda+\varepsilon} \quad (\lambda=1,2,\cdots,7), \tag{58}$$

$$\int |S_9|^{882}\mathrm{d}\alpha \ll P^{853+\varepsilon}, \tag{59}$$

$$\int |S_9|^{882+256\lambda}\mathrm{d}\alpha \ll P^{853+255\lambda+\varepsilon} \quad (\lambda=1,2,\cdots,8). \tag{60}$$

2.20. $B(9)$ 的证明. 我们有

$$\int |C_9|^{20+16\lambda}\mathrm{d}\alpha \ll P^{10+15\lambda+\varepsilon} \quad (\lambda=1,\cdots,5), \tag{61}$$

$$\int |C_9|^{100+32\lambda}\mathrm{d}\alpha \ll P^{85+31\lambda+\varepsilon} \quad (\lambda=1,\cdots,6), \tag{62}$$

$$\int |C_9|^{292+64\lambda}\mathrm{d}\alpha \ll P^{271+63\lambda+\varepsilon} \quad (\lambda=1,\cdots,7), \tag{63}$$

$$\int |C_9|^{740+128\lambda}\mathrm{d}\alpha \ll P^{712+127\lambda+\varepsilon} \quad (\lambda=1,\cdots,8), \tag{64}$$

$$\int |C_9|^{1764+256\lambda}\mathrm{d}\alpha \ll P^{1738+255\lambda+\varepsilon} \quad (\lambda=1,\cdots,9). \tag{65}$$

2.21. $A(10)$ 的证明. 我们有

$$\int |S_{10}|^{20+16\lambda}\mathrm{d}\alpha \ll P^{10+15\lambda+\varepsilon} \quad (\lambda=1,\cdots,5), \tag{66}$$

$$\int |S_{10}|^{100+32\lambda}\mathrm{d}\alpha \ll P^{85+31\lambda+\varepsilon} \quad (\lambda=1,\cdots,6), \tag{67}$$

$$\int |S_{10}|^{292+64\lambda}\mathrm{d}\alpha \ll P^{271+63\lambda+\varepsilon} \quad (\lambda=1,\cdots,7), \tag{68}$$

$$\int |S_{10}|^{740+128\lambda}\mathrm{d}\alpha \ll P^{712+127\lambda+\varepsilon} \quad (\lambda=1,\cdots,8), \tag{69}$$

$$\int |S_{10}|^{2020}\mathrm{d}\alpha \ll P^{1983+\varepsilon}, \tag{70}$$

$$\int |S_{10}|^{2020+512\lambda}\mathrm{d}\alpha \ll P^{1983+511\lambda+\varepsilon} \quad (\lambda=1,\cdots,9). \tag{71}$$

2.22. $B(10)$ 的证明. 作为 (8) 式的一个显然推论, 我们有

$$\int |C_{10}|^{38}\mathrm{d}\alpha \ll P^{27+\varepsilon}.$$

此外, 有

$$\int |C_{10}|^{38+16\lambda}\mathrm{d}\alpha \ll P^{27+15\lambda+\varepsilon} \quad (\lambda = 1, \cdots, 4), \tag{72}$$

$$\int |C_{10}|^{102+32\lambda}\mathrm{d}\alpha \ll P^{87+31\lambda+\varepsilon} \quad (\lambda = 1, \cdots, 6), \tag{73}$$

$$\int |C_{10}|^{294+64\lambda}\mathrm{d}\alpha \ll P^{273+63\lambda+\varepsilon} \quad (\lambda = 1, \cdots, 7), \tag{74}$$

$$\int |C_{10}|^{742+128\lambda}\mathrm{d}\alpha \ll P^{714+127\lambda+\varepsilon} \quad (\lambda = 1, \cdots, 8), \tag{75}$$

$$\int |C_{10}|^{1766+256\lambda}\mathrm{d}\alpha \ll P^{1730+255\lambda+\varepsilon} \quad (\lambda = 1, \cdots, 9), \tag{76}$$

$$\int |C_{10}|^{4070+512\lambda}\mathrm{d}\alpha \ll P^{4025+511\lambda+\varepsilon} \quad (\lambda = 1, \cdots, 10). \tag{77}$$

## 3. 应　　用

本节中, 我要谈一谈关于定理的一些可能的应用.

1) Tarry 问题. 我希望在以后的文章中讨论这个问题.

2) 华林问题. 设 $G(k)$ 为最小的正整数 $s$, 使得对于所有充分大的正整数 $N$, 方程

$$N = x_1^k + \cdots + x_s^k, \quad x_\nu \geqslant 0$$

总可解. Vinogradov 曾经证明了

$$G(k) < 4k\log k + 8k\log\log k + 12k.$$

如果引入本节的结果, 并按照 Vinogradov 同样的方法, 我们可以在 $k \leqslant 15,000$ 时得到比他更好的结果.

3) 三角和估计. 我们改进了 Vinogradov①的一些结果, 细节将另文发表.

4) 联立华林问题. 设 $T$ 为方程组

$$x_1^h + \cdots + x_s^h = N_h \quad (h = 1, 2, \cdots, k)$$

的正整数解的个数. 假如 $s$ 由引言中的表格给出, 则本文的结果可以推出

$$T = O(P^{s-\frac{1}{2}k(k+1)+\varepsilon}).$$

关于 $T$ 与多重 Fourier 积分和同余式的一些定理之间的精确关系, 我们将另文给出.

(贾朝华　译)

---

① 见 85 页的脚注②和③, 以及 *Bull.de l'Acad.des Sciences de l'U.R.S.S.*, 1938: 399–416.

# 关于一个指数和①

华罗庚

本文的主要目的为证明下面定理:

命 $f(x)$ 为一个 $k$ 次整系数多项式.

$$f(x) = a_k x^k + \cdots + a_1 x$$

及命 $(a_k, \cdots, a_1, q) = 1$, 则

$$S(q, f(x)) = \sum_{x=1}^{q} e_q(f(x)) = O(q^{1-1/k+\varepsilon}), \quad e_q(z) = e^{2\pi i z/q},$$

此处与 $O$ 有关的常数仅依赖于 $k$ 与 $\varepsilon$.

这一结果比我先前的一个结果为优②, 在该结果中与 $O$ 有关的常数还要依赖于多项式的系数.

在 §§3, 4 中, 我们将给出定理一些简单应用, 这一定理的另外一个应用为用于 Vinogradov 研究过的一个问题, 将于另文发表.

§1. 定理为下面引理的推论:

**基本引理** 命 $l > 1$ 及 $p$ 为一个素数, 又命

$$f(x) = a_k x^k + \cdots + a_1 x$$

及 $p \nmid (a_1, \cdots, a_k)$, 则

$$S(p^l, f(x)) = O(p^{l(1-\frac{1}{k})}),$$

此处与 $O$ 有关的常数仅依赖于 $k$.

引理的证明将在下一节中给出.

**引理 1** (Mordell)③

$$S(p, f(x)) = O(p^{1-1/k}).$$

**引理 2** 若 $(q_1, q_2) = 1$ 及 $f(0) = 0$, 则

$$S(q_1 q_2, f(x)) = S(q_1, f(q_2 x)/q_2) S(q_2, f(q_1 x)/q_1).$$

---

① 1939 年 4 月 14 日收到. *J. Chinese Math. Soc.*, 1940, 2: 301–312.

② *Jour. of London Math. Soc.*, 1938, 13: 54–64.

③ *Quarterly Jour.*, 1932, 3: 161–167.

**证明** 记 $x=q_1y+q_2z$, 则 $y$ 与 $z$ 分别过 $\bmod q_2$ 与 $\bmod q_1$ 的完全剩余系时, $x$ 过 $\bmod q_1q_2$ 的一个完全剩余系. 进而言之, 我们有恒等式

$$e_{q_1q_2}(f(q_1y+q_2z))=e_{q_1}(f(q_2y)/q_2)e_{q_2}(f(q_1z)/q_1).$$

所以

$$\begin{aligned}S(q_1q_2,f(x))&=\sum_{x=0}^{q_1q_2-1}e_{q_1q_2}(f(x))\\&=\sum_{y=0}^{q_2-1}e_{q_2}(f(q_1y)/q_1)\sum_{z=0}^{q_1-1}e_{q_1}(f(q_2z)/q_2)\\&=S(q_1,f(q_2x)/q_2)S(q_2,f(q_1x)/q_1).\end{aligned}$$

**定理 1** 若 $(a_1,\cdots,a_k,q)=1$, 则

$$S(q,f(x))=O(q^{1-1/k+\varepsilon}).$$

**证明** 由基本引理及引理 1 与 2, 我们有

$$|S(q_1f(x))|\leqslant(c(k))^{v(q)}q^{1-1/k},$$

此处 $v(q)$ 表示 $q$ 的不同素因子个数, 由于

$$c(k)^{v(q)}=O(q^{\varepsilon}),$$

所以定理成立.

**§2 定义** 命

$$f(x)=a_kx^k+\cdots+a_1x$$

$p^{l_s}\|sa_s,t=\min(l_1,\cdots,l_k),t\geqslant 0$. 命 $s$ 为满足 $p^t\|sa_s$ 最大之整数, 这一整数定义为 $f(x)$ 的指标, 并记为 $s=\mathrm{ind}f(x)$. 我们立即得到下面诸引理.

**引理 1**

$$\mathrm{ind}f(x)=\mathrm{ind}f(x+\lambda).$$

**引理 2**

$$\mathrm{ind}f(x)\geqslant\mathrm{ind}f(px).$$

**引理 3** 若 $\mathrm{ind}f(x)=\mathrm{ind}f(px)$, 则由

$$f'(x)\equiv 0(\bmod p^{t+1})$$

可以导出 $p|x$.

**证明** 对于任何 $s'$, 由定义有 $l_s \leqslant l_{s'}$ 及 $l_s + s \leqslant l_{s'} + s'$. 所以

$$l_s < l_{s'}, \quad 当\ s \neq s';$$

事实上, 若 $s < s'$, 则这一结果是定义的简单推论. 若 $s > s'$, 则 $l_s \leqslant l_{s'} + s' - s < l_{s'}$, 所以由 $f'(x) \equiv 0(\bmod p^{t+1})$ 推出

$$sa_s x^{s-1} \equiv 0(\bmod p^{t+1}),$$

即 $p|x$.

**基本引理的证明** 由于

$$|S(p^t, f(x))| \leqslant p^l \leqslant p^{t+1} \leqslant p^{2t} \leqslant k^2, \quad 当\ t > 0$$

及由 Mordell 引理,

$$S(p, f(x)) = 0(p^{1-1/k}), \quad 当\ t = 0$$

所以当 $l \leqslant t + 1$ 时, 引理成立. 因此我们可以假定 $l \geqslant t + 2$,

$$\lambda_1, \cdots, \lambda_e$$

为同余式

$$f'(x) \equiv 0(\bmod p^{t+1})$$

的不同根, 则显然 $e \leqslant p^t k \leqslant k^2$ 及

$$\sum_{x=1}^{p^l} e_{p^l}(f(x)) = \sum_{\substack{i=1 \\ x\equiv i}}^{p^{t+1}} \sum_{\substack{x=1 \\ (p^{t+1})}}^{p^l} e_{p^l}(f(x)).$$

若 $i$ 不等于 $\lambda's$ 中的任何一个, 则命 $x = y + p^{l-t-1}z$. 我们得到

$$\sum_{\substack{x=1 \\ x\equiv i(p^{t+1})}}^{p^l} e_{p^l}(f(x)) = \sum_{\substack{y=1 \\ y\equiv i(p^{t+1})}}^{p^{l-t-1}} e_{p^l}(f(y)) \sum_{\substack{z=1 \\ f'(y)\not\equiv 0,(p^{t+1})}}^{p^{t+1}} e_{p^{t+1}}(zf'(y)) = 0.$$

所以

$$\left|\sum_{x=1}^{p^l} e_{p^l}(f(x))\right| = \left|\sum_{\substack{l=1 \\ x\equiv\lambda_i,(p^{t+1})}}^{e} \sum_{x=1}^{p^l} e_{p^l}(f(x))\right|$$

$$= e \max_{l\leqslant i\leqslant e} \left|\sum_{y=1}^{p^{l-t-1}} e_{p^l}(f(\lambda_i + p^{t+1}y) - f(\lambda_i))\right|$$

$$= e \max_{2 \leqslant i \leqslant e} \left| \sum_{x=1}^{p^{l-t-1}} e_{p^{l-\mu_i}}(g_i(x)) \right|,$$

此处 $p^{\mu_i}$ 为能整除 $f(\lambda_i+p^{t+1}y)-f(\lambda_i)$ 所有系数的 $p$ 的最高幂次, 由于 $\mu_i \leqslant k(1+t)$, 所以

$$\begin{aligned} \left| \sum_{x=1}^{p^l} e_{p^l}(f(x)) \right| &\leqslant e \max_{1 \leqslant i \leqslant e} p^{\mu_i - t - 1} \left| \sum_{x=1}^{p^{l-\mu_i}} e_{p^{l-\mu_i}}(g_i(x)) \right| \\ &\leqslant k^2 \max_{1 \leqslant i \leqslant e} p^{\mu_i(1-1/k)} \left| \sum_{x=1}^{p^{l-\mu_i}} e_{p^{l-\mu_i}}(g_i(x)) \right|, \end{aligned} \tag{1}$$

若 $\text{ind} f(x) = \text{ind} f(px)$, 则由引理 3 得

$$\begin{aligned} \sum_{x=1}^{p^l} e_{p^l}(f(x)) &= p^{l+1} \sum_{y=1}^{p^{l-t-1}} e_{p^l}(f(y)) \\ &= p^{t+1} \sum_{y=1}^{p^{l-t-2}} e_{p^l}(f(py)) \\ &= p^{t+1} \sum_{y=1}^{p^{l-t-2}} e_{p^l-\mu}(g(x)) \\ &= p^{\mu-1} \sum_{y=1}^{p^{l-\mu}} e_{p^l-\mu}(g(y)), \end{aligned}$$

此处 $p^\mu$ 为能整除 $f(py)$ 所有系数的 $p$ 的最高幂次及 $f(py) = p^\mu g(y)$. 则得

$$\left| \sum_{x=1}^{p^l} e_{p^l}(f(x)) \right| \leqslant p^{\mu(1-1/k)} \left| \sum_{x=1}^{p^{l-\mu}} e_{p^{l-\mu}}(g(x)) \right|. \tag{2}$$

若我们反复运用这一方法, 则最多有 $k$ 步, 而每次均有一个小于 $k^2$ 的因子 (用 (1)), 其他的则仅给出一个因子 1(由 (2)), 所以

$$S(p^l, f(x)) = O(p^{l(1-1/k)}).$$

附记: 定理中的 $\varepsilon$ 在绝大多数情况下都是可以省略的, 更仔细地讲, 假定 $k$ 非形式 $2^g$ 或 $3.2^g$, 则对基本引理的证明作一点修正并用 Davenport① 一条引理可得

$$S(q^l, f(x)) = O(q^{1-1/k}).$$

① *Jour. für Mach.*, 1933, 169: 158-176.

§3 本节的目的为证明下面定理

**定理 1**　命

$$f(x) = a_k x^k + \cdots + a_1 x, \quad (q_k, \cdots, a_1, q) = 1,$$

则

$$\sum_{x=1}^{m} e_q(f(x)) = \frac{m}{q} S(q, f(x)) + O(q^{1-1/k+\varepsilon}).$$

显然只要证明下面的事实即足：若 $0 < m < q$, 则

$$\sum_{x=1}^{m} e_q(f(x)) = O(q^{1-1/k+\varepsilon}).$$

首先, 我们寻找一个有周期 $q$ 的函数 $g(x)$, 且满足

$$g(x) = \begin{cases} 1, & 当\ 0 < x < m, \\ 0, & 当\ m < x < q. \end{cases}$$

若我们假定 $g(0) = g(m) = \frac{1}{2}$, 则 $g(x)$ 可以表示为 Fourier 级数:

$$g(x) = \frac{m}{q} + \sum_{n=-\infty}^{\infty}{}' \frac{1}{2\pi i n}(e_q(nx) - e_q(n(x-m))),$$

此处在求和号中需去掉 $n = 0$ 对应之项, 命

$$S_{q'} = \sum_{n=q+1}^{q'} e_q(nx).$$

熟知若 $x$ 非 $q$ 之倍数, 则

$$S_{q'} \leqslant \frac{1}{2} \left\{ \frac{x}{q} \right\}^{-1},$$

此处 $\{t\}$ 表示 $t$ 至其最近整数之距离. 从而, 由分部求和法得

$$\sum_{n=q+1}^{q'} \frac{1}{n} e_q(\pm nx) = O\left( \frac{1}{q\{x/q\}} \right).$$

类似地, 若 $x \neq m$ 及 $0 < x < q$, 则

$$\sum_{n=q+1}^{q'} \frac{1}{n} e_q(\pm(x-m)n) = O\left( \frac{1}{q\{(x-m)/q\}} \right).$$

当 $x \neq m$ 及 $0 < x < q$ 时, 我们有

$$\begin{aligned} g(x) = \frac{m}{q} + \sum_{n=-q}^{q}{}' \frac{1}{2\pi i n}(e_q(nx) - e_q(n(x-m))) \\ + O\left(\frac{1}{q\{x/q\}}\right) + O\left(\frac{1}{q\{(x-m)/q\}}\right). \end{aligned} \tag{3}$$

其次

$$\sum_{x=1}^{m} e_q(f(x)) = \sum_{x=1}^{q}{}^{*} e_q(f(x))g(x) + O(1)$$

此处 $\sum^*$ 表示在求和号中除掉 $x = m$ 与 $x = q$, 由 (3) 即得

$$\begin{aligned} \sum_{x=1}^{m} e_q(f(x)) = &\frac{m}{q}\sum_{x=1}^{q}{}^{*} e_q(f(x)) + \frac{1}{2\pi i}\sum_{n=-q}^{q}{}' \frac{1}{n} \\ &\times \left(\sum_{x=1}^{q}{}^{*} e_q(f(x)+nx) - \sum_{x=1}^{q}{}^{*} e_q(f(x)+nx-mn)\right) \\ &+ O\left(\sum_{x=1}^{q}{}^{*} \frac{1}{q\{x/q\}}\right) + O\left(\sum_{x=1}^{q}{}^{*} \frac{1}{q\{(x-m)/q\}}\right) \\ = &I_1 + I_2 + I_3 + I_4 + I_5 \quad (\text{定义}), \end{aligned}$$

我们有

$$I_4 = \sum_{x=1}^{q}{}^{*} \frac{1}{q\{x/q\}} \leqslant \frac{1}{q}\sum_{x=1}^{q/2} \frac{2q}{x} = O(\log q),$$

及 $I_5$ 满足同样的估计.

最后, 考虑

$$\sum_{n=1}^{q} \frac{1}{n} \sum_{x=1}^{q} e_q(f(x) + nx).$$

命 $(a_k, \cdots, a_2, q) = q'$ 及 $q''$ 为 $q'$ 的任何因子, 我们将 $n$ 适合条件

$$(a_k, \cdots, a_2, a_1 + n, q) = q''$$

的诸项集合起来, 则

$$\begin{aligned} &\sum_{n=1}^{q} \frac{1}{n} \left|\sum_{x=1}^{q} e_q(f(x) + nx)\right| \\ \leqslant &\sum_{q''/q} \sum_{\substack{n=1 \\ a_1+n\equiv 0,(q'')}}^{q} \frac{1}{n} \left|\sum_{x=1}^{q} e_{q/q''}\left(\frac{1}{q''}f(x) + nx\right)\right| \end{aligned}$$

$$= O\left[\sum_{q''/q}\sum_{\substack{n=1\\ a_1+n\equiv 0,(q'')}}^{q}\frac{1}{n}q''(q/q'')^{1-1/k+\varepsilon}\right]$$
$$= O\left(\sum_{q''/q}\sum_{m=1}^{q/q''}\frac{1}{mq''}q''(q/q'')^{1-1/k+\varepsilon}\right)$$
$$= O\left(q^{1-1/k+\varepsilon}\log q\sum_{q''/q}q''^{-1+1/k+\varepsilon}\right)$$
$$= O(q^{1-1/k+\varepsilon}).$$

这一方法给出

$$I_2 = O(q^{1-1/k+\varepsilon}),\quad I_3 = O(q^{1-1/k+\varepsilon}).$$

显然

$$I_1 = O(q^{1-1/k+\varepsilon}).$$

将所有这些结果综合起来, 即得定理 1.

由于 $k$ 次整值多项式的分母 $\leqslant k!$, 若我们仅假定 $f(x)$ 为一个 $k$ 次整值多项式及 $f(x)\not\equiv f(0)(\mathrm{mod} p)$, 此处 $p$ 为 $q$ 的任何因子, 定理 1 成立.

§4. 最后, 我们将证明一条定理, 它对 Waring 问题的"优弧"问题有一个有趣的应用.

**定理 2** 命 $f(x)$ 为一个整值多项式, 命

$$S(\alpha)=\sum_{x=0}^{P}\mathrm{e}^{2\pi\mathrm{i}f(x)\alpha},\quad \alpha=\frac{a}{q}+\beta,$$

$$I(\beta)=\int_0^P \mathrm{e}^{2\pi\mathrm{i}f(x)\beta}\mathrm{d}x,$$

则当 $q=O(P^{1-\varepsilon})$ 及 $|\beta|=O(q^{-1}P^{-k+1-\varepsilon})$ 时, 有

$$S(\alpha)=\overline{q}^{-1}S_{a,q}I(\beta)+O(q^{1-1/k+\varepsilon}),$$

此处 $\overline{q}=q(q,d)$ 及 $d$ 为 $f(x)$ 的系数的最小公分母,

$$S_{a,q}=\sum_{x=1}^{q}e_q(\alpha f(x)),$$

及与 $O$ 有关的常数仅依赖于 $f(x)$ 的系数.

欲证这一定理, 我们将应用著名的 Euler 求和公式:

定义

$$b_1(x)=x-[x]-\frac{1}{2},$$

此处 $[x]$ 表示不超过 $x$ 的最大整数. 我们用归纳法定义 $b_l(x)$,

$$b_l(x+1)=b_l(x) \tag{4}$$

及

$$\int_0^x b_l(y)\mathrm{d}y=b_{l+1}(x)-b_{l+1}(0). \tag{5}$$

命 $b>a$ 及 $g(x)$ 与其导数 (以下所出现者) 在区间 $a\leqslant x\leqslant b$ 中为连续函数, 则对于任何 $t$ 皆有

$$\sum_{\substack{m\\ a\leqslant m+t<b}} g(m+t)=\int_a^b g(x)\mathrm{d}x+\sum_{r=0}^{l-1}\{g^{(r)}(b)b_{r+1}(t-b)-g^{(r)}(a)b_{r+1}(t-a)\}$$
$$-\int_a^b g^{(l)}(x)b_l(t-x)\mathrm{d}x.$$

**定理的证明** 第一步:

$$S(\alpha)=\sum_{x=0}^{P}\mathrm{e}^{2\pi\mathrm{i}f(x)\alpha}=\sum_{v=1}^{\overline{q}}\sum_{\substack{0\leqslant r\leqslant P\\ r\equiv v,(\overline{q})}} e_q(af(v))\mathrm{e}^{2\pi\mathrm{i}\beta f(r)}$$
$$=\sum_{v=1}^{\overline{q}} e_q(af(v))d_v,$$

此处

$$d_v=\sum_{\substack{j\\ 0\leqslant\overline{q}j+v\leqslant p}}\mathrm{e}^{2\pi\mathrm{i}\beta f(\overline{q}j+v)}=\sum_{\substack{j\\ 0\leqslant j+v/\overline{q}\leqslant P/q}}\Phi(j+v/\overline{q}),\quad \Phi(x)=\mathrm{e}^{2\pi\mathrm{i}\beta f(\overline{q}x)}.$$

由 Euler 求和公式得

$$d_v=\int_0^{p/\overline{q}}\Phi(x)\mathrm{d}x+\sum_{r=1}^{l-1}\left\{\Phi^{(r)}\left(\frac{p}{\overline{q}}\right)b_{r+1}\left(\frac{v}{\overline{q}}-\frac{P}{\overline{q}}\right)\right.$$
$$\left.-\Phi^{(r)}(0)b_{r+1}\left(\frac{v}{\overline{q}}\right)\right\}-\int_0^{p/\overline{q}}\Phi^{(l)}(x)b_l\left(\frac{v}{\overline{q}}-x\right)\mathrm{d}x. \tag{6}$$

由于

$$\int_0^{P/\overline{q}}\Phi(x)\mathrm{d}x=\int_0^{p/\overline{q}}\mathrm{e}^{2\pi\mathrm{i}\beta f(\overline{q}x)}\mathrm{d}x=\frac{1}{\overline{q}}\int_0^p\mathrm{e}^{2\pi\mathrm{i}\beta f(y)}\mathrm{d}y,$$

所以由 (5), (6) 可知

$$S(a)=\frac{S_{aq}}{q}I(P)+\sum_{r=1}^{l}\left\{\Phi^{(r)}\left(\frac{P}{\overline{q}}\right)a_{r+1}\left(\frac{v}{\overline{q}}-\frac{P}{\overline{q}}\right)\right.$$
$$\left.-\Phi^{(r)}(0)b_{r+1}\left(\frac{v}{\overline{q}}\right)\right\}-R,$$

此处

$$a_{r+1}\left(\frac{v}{\overline{q}}-t\right)=\sum_{v=1}^{\overline{q}}e_q(af(v))b_{r+1}\left(\frac{v}{\overline{q}}-t\right),$$

$$R=\sum_{v=1}^{\overline{q}}e_q(af(v))\int_0^{P/\overline{q}}\Phi^{(l)}(x)b_l\left(\frac{v}{\overline{q}}-x\right)\mathrm{d}x.$$

第二步：若 $q=O(P^{1-\varepsilon}),\beta=O(q^{-1}P^{-k+1-\varepsilon})$ 及 $0\leqslant x\leqslant P/\overline{q}$, 则

$$\Phi^{(r)}=O(P^{-r\varepsilon}).\tag{7}$$

假定 $f(v)$ 仅含一项, 即 $f(v)=Av^k$, 命

$$\Psi(x)=\mathrm{e}^{2\pi\mathrm{i}\beta A(\overline{q}x)^k},$$

首先, 我们将证明

$$\Psi^{(r)}=O(P^{-r\varepsilon}).$$

命 $\Psi_1(z)=\mathrm{e}^{z^k}$, 则

$$\Psi_1^{(r)}(z)=\mathrm{e}^{z^k}F_r(z),$$

此处 $F_r(z)$ 为一个 $r(k-1)$ 次多项式, 所以

$$\Psi^{(r)}(x)=\mathrm{e}^{2\pi\mathrm{i}\beta A(\overline{q}x)^k}F_r((2\pi\mathrm{i}\beta A)^{1/k}\overline{q}x)((2\pi\mathrm{i}\beta A)^{1/k}\overline{q})^r.$$

从而

$$\Psi^{(r)}(x)=O(1+(|\beta|^{1/k}qx)^{(k-1)r})(|\beta|^{1/k}q)^r=O(p^{-r\varepsilon}).$$

其次, 我们假定 $f(x)$ 为一个多项式, 其首项系数为 $A$. 命

$$\Phi(x)=\Psi(x)\Psi_1(x),\quad \Psi_1(x)=\mathrm{e}^{2\pi\mathrm{i}\beta(f(\overline{q}x)-A(\overline{q}x)^k)}.$$

假定 (7) 对于 $k-1$ 真实, 即当 $|\beta|\leqslant q^{-1}P^{-k+2-\varepsilon}$ 时, 有

$$\Psi_1^{(r)}(x)=O(P^{-r\varepsilon}).$$

由于 $q^{-1}P^{-k+2-\varepsilon} > q^{-1}P^{-k+1-\varepsilon}$, 所以当 $|\beta| = O(q^{-1}p^{-k+1-\varepsilon})$ 时, 有

$$\Psi_1^{(r)}(x) = O(P^{-r\varepsilon}).$$

进而言之, 由于

$$\Phi^{(r)}(x) = \Psi^{(r)}(x)\Psi_1(x) + \begin{pmatrix} r \\ 1 \end{pmatrix} \Psi^{(r-1)}(x)\Psi_1'(x) + \cdots + \Psi(x)\Psi_1^{(r)}(x),$$

所以

$$\Phi^{(r)}(x) = O(\max_{0\leqslant i\leqslant r}(\Psi^{(r-i)}(x)\Psi_1^{(i)}(x))) = O(P^{-r\varepsilon}).$$

第三步：取

$$l = [1/\varepsilon] + 1,$$

则

$$\Phi^{(l)}(x) = O(P^{-1}).$$

所以

$$|R| = O\left(\frac{1}{q}\int^{P/\overline{q}} P^{-1}\mathrm{d}x\right) = O(1).$$

第四步：命

$$S_v = \sum_{h=1}^{v} e_q(af(h)).$$

由 $a_v(t)$ 的定义可知

$$\begin{aligned} a_r\left(\frac{v}{\overline{q}} - t\right) &= S_1 b_{r+1}\left(\frac{1}{\overline{q}} - t\right) \\ &\quad + \sum_{v=2}^{\overline{q}}(S_v - S_{v-1})b_{r+1}\left(\frac{v}{\overline{q}} - t\right) \\ &= \sum_{m=1}^{\overline{q}-1} S_m\left\{b_{r+1}\left(\frac{m}{\overline{q}} - t\right) - b_{r+1}\left(\frac{m+1}{\overline{q}} - t\right)\right\} + S_q b_{r+1}(1-t). \end{aligned}$$

由定理 1 可知

$$S_v = O(\overline{q}^{1-1/k+\varepsilon}), \quad 当\ 0 < v \leqslant q.$$

所以

$$a_r\left(\frac{v}{\overline{q}} - t\right) = 0\left(\overline{q}^{1-1/k+\varepsilon}\left\{\sum_{m=1}^{\overline{q}-1}\left|b_{r+1}\left(\frac{m}{\overline{q}} - t\right) - b_{r+1}\left(\frac{m+1}{\overline{q}} - t\right)\right| + 1\right\}\right).$$

由于 $b_{r+1}$ 是一个有界变差函数, 所以

$$a_r\left(\frac{v}{\overline{q}}-t\right)=O(\overline{q}^{1-1/k+\varepsilon}).$$

第五步: 联合第二, 第三与第四步的结果, 我们最后得到

$$s(\alpha)-\overline{q}^{-1}S_{aq}I(P)=O\left(\overline{q}^{1-1/k+\varepsilon}\sum_{r=1}^{l-1}P^{-r\varepsilon}+1\right)=O(\overline{q}^{1-/k+\varepsilon}).$$

(王元　译)

# 一个数分拆为互不相等数之和的分拆个数[①②]

华罗庚 (昆明, 国立清华大学)

## 1. 导　　言

命 $q(n)$ 表示将一个整数分拆为不相等数之和或奇数之和的分拆个数[③], 则

$$f(x) = 1 + \sum_{n=1}^{\infty} q(n)x^n = (1+x)(1+x^2)(1+x^3)\cdots$$
$$= \frac{1}{(1-x)(1-x^3)(1-x^5)\cdots}. \tag{1.1}$$

Hardy 与 Ramanujan[④]指出, 用他们的基本分析方法可以得到如下结果:

$$q(n) = \frac{1}{2^{1/2}}\frac{\mathrm{d}}{\mathrm{d}n}J_0\left[\mathrm{i}\pi\left\{\frac{1}{3}\left(n+\frac{1}{24}\right)\right\}^{1/2}\right] + 2^{1/2}\cos\left(\frac{2}{3}\pi n - \frac{1}{9}\pi\right)\frac{\mathrm{d}}{\mathrm{d}n}J_2$$
$$\times\left[\frac{1}{3}\mathrm{i}\pi\left\{\frac{1}{3}\left(n+\frac{1}{24}\right)\right\}^{1/2}\right] + \cdots + \text{to } [\alpha n^{1/2}] \text{ terms} + O(1),$$

此处 $\alpha$ 为任意常数, 相比于 $n$ 的分拆个数 $p(n)$ 的估计, 这一结果是欠满意的. 这是由于在 $p(n)$ 的情况下, 当 $n$ 递增时, 误差项趋于 0, 最近 Rademacher[⑤] 获得了关于 $p(n)$ 的一个等式, 本文的工作为直接应用 Hardy-Ramanujan 方法, 再加上两点改进, 即 Kloosterman 和与 Rademacher 的"无穷级 Farey 分割"的应用.

本文方法也可以用来寻求

$$\sum_{x=1}^{[n^{1/2}]} p(n-x^2)$$

的显公式, 其中 $p(n)$ 表示 $n$ 的非限制分拆数.

---

① 1940 年 4 月 27 日提交给学会; 编者收到日期为 1941 年 1 月 9 日. *Tras. Amer. Math. Soc.*, 1942, 51: 194-201

② 本文在二战前已被*Acta Arithmetica* 接受.

③ *Cf. MacMahon, Combinatory Analysis*, 1916, 2: 11.

④ *Proceedings of the London Mathematical Society*(2), 1918, 17: 75–115.

⑤ *Proceedings of London Mathematical Society*(2), 1937, 43: 241–254.

## 2. 结果的陈述

命

$$\varepsilon_{h,k}=\begin{cases}\exp\Big(-\pi i\Big(\frac{(h'^2-1)}{8}\Big(\frac{1-hh'}{k}-1\Big)+\frac{h'(1-hh')}{8k}\\ \quad+\frac{1}{24}\Big(k+\frac{1-hh'}{k}\Big)(hh'^2-h'-h)\Big)\Big), & \text{当}2|k,\\ \exp\Big(\frac{\pi i}{24}\Big(k+\frac{1-hh'}{k}\Big)(h+h'-h^2h')\Big), & \text{当}2\nmid k,2\nmid h,\\ \exp\Big(-\frac{\pi i}{8}\Big(k^2-1-hk+\frac{1}{3}(h+h')\Big(hh'k-\frac{hh'-1}{k}\Big)\Big)\Big), \\ & \text{当}2\nmid k,2|h,\end{cases}$$

及

$$\omega_{h,k}=\begin{cases}\varepsilon_{h,k}\exp\left(-\frac{\pi i}{12k}(h+h')\right), & \text{当 } 2|k\\ \varepsilon_{h,k}\exp\left(-\frac{\pi i}{24k}(2h-h')\right), & \text{当 } 2\nmid k,\end{cases}$$

此处 $hh'\equiv 1(\mathrm{mod} k), h\equiv h'(\mathrm{mod} 2)$.

**定理**　一个整数分拆为互不相等数之和的分拆个数为

$$q(n)=\frac{1}{2^{1/2}}\sum_{k=1,k\ odd}^{\infty}\sum_{(h,k)=1,0<h\leqq k}\omega_{h,k}e^{-2\pi ihn/k}\frac{d}{dn}J_0\left(\frac{i\pi}{k}\left\{\frac{2}{3}\left(n+\frac{1}{24}\right)\right\}^{1/2}\right),$$

此处 $J_0(x)$ 为 $O$ 级 Bessel 函数.

## 3. Farey 分割

关于 (1.1), 由 Caucly 积分公式得

$$q(n)=\frac{1}{2\pi i}\int_C\frac{f(x)}{x^{n+1}}dx.$$

积分路往为圆周 $|x|=e^{-2\pi N^{-2}}$, 此处 $N$ 为由我们派定的某正整数, 通常的方法为将圆周分成 $N$ 级 Farey 弧 $\xi_{h,k}$. Farey 弧 $\xi_{h,k}$ 由

$$x=\exp(2\pi ih/k-2\pi N^{-2}+2\pi i\vartheta),\quad (h,k)=1,\tag{3.1}$$

与

$$-\vartheta_1(h,k)=\frac{h+h_1}{k+k_1}-\frac{h}{k}\leqslant\vartheta\leqslant\frac{h+h_2}{k+k_2}-\frac{h}{k}=\vartheta_2(h,k)\tag{3.2}$$

定义, 其中 $h_1/k_1, h/k, h_2/k_2$ 为 $N$ 级 Farey 序列中的三个连续分数, 熟知

$$\frac{1}{k(N+k)} \leqslant \vartheta_1(h,k) < \frac{1}{k(N+1)},$$
$$\frac{1}{k(N+k)} \leqslant \vartheta_2(h,k) < \frac{1}{k(N+1)}. \tag{3.3}$$

所以我们得

$$q(n) = \frac{1}{2\pi i} \sum_{(h,k)=1, 0<h\leqslant k\leqslant N} \int_{\xi_{h,k}} \frac{f(x)}{x^{n+1}} dx. \tag{3.4}$$

命 $I_1$ 与 $I_2$ 分别表示适合 $2|k$ 与 $2\nmid k$ 的诸项之和, 则由 (3.4) 可知

$$q(n) = I_1 + I_2. \tag{3.5}$$

## 4. 关于 Kloosterman 和之诸引理

**引理 4.1**[①] 命

$$g(N,\vartheta,h,k) = \begin{cases} 1, & 当 -\vartheta_1(h,k) \leqslant \vartheta \leqslant \vartheta_2(h,k), \\ 0, & 其他情形, \end{cases}$$

则

$$g = \sum_{r=1}^{k} b_r e^{2\pi i r h'/k}$$

此处 $h'$ 为适合

$$hh' \equiv l(\bmod k)$$

之整数, $b_r$ 独立于 $h$ 及

$$\sum_{r=1}^{k} |b_r| < \log 4k.$$

**引理 4.2** 命 $a$ 为一个绝对常数, 则

$$\sum_{0<h\leqslant ak, (h,ak)=1, h\equiv l(a)} \exp\left(\frac{2\pi i}{ak}(nk+mh')\right) = O(k^{2/3+\varepsilon}(n,k)^{1/3}).$$

**引理 4.3** 若 $k$ 为偶数及 $\omega_{h,k}$ 由 §2 定义, 则

$$S_k = \sum_{1\leqslant h\leqslant k, (h,k)=1, hh'\equiv 1(k)} \omega_{h,k} e^{2\pi i(nh+mh')/k} = O(k^{2/3+\varepsilon}(n,k)^{1/3}).$$

---

① T. Estermann. Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, 1929, 7: 93, 94.

**证明**　为简单计, 在此我仅给出情况 $24k$ 的证明, 则

$$S_k = \sum_{1\leqslant l\leqslant 24,(l,24)=1}\ \sum_{1\leqslant h\leqslant k,(h,k)=1,hh'\equiv 1,h\equiv l(24)} \omega_{h,k}\mathrm{e}^{2\pi\mathrm{i}(nh+mh')/k}.$$

内和变成如引理 4.2 所示的 Kloosterman 和. 所以

$$S_k = O(k^{2/3+\varepsilon}(n,k)^{1/3}).$$

关于另外情况的证明, 并无困难, 但略为复杂一点. 下面的事实将被用到: 命

$$F(h,k) = \omega_{h,k}\mathrm{e}^{2\pi\mathrm{i}(nh+mh')/k},$$

则 $F(h+k,k) = F(h,k)$.

**引理 4.4**　命 $2\nmid k$ 及 $\omega_{h,k}$ 如 §2 所定义, 则

$$\begin{aligned} S &= \sum_{1\leqslant h\leqslant k,(h,k)=1,hh'\equiv 1(k),h'\text{odd}} \omega_{h,k}\mathrm{e}^{\pi\mathrm{i}(2nh+mh')/k} \\ &= O(k^{2/3+\varepsilon}(h,k)^{1/3}). \end{aligned}$$

**证明**　类似于引理 4.3 的证明, 在此仅需注意

$$S = \sum_{1\leqslant h<2k,(h,2k)=1,hh'\equiv 1(2k)} \cdots.$$

## 5. 关于椭圆模函数线性变换的引理

**引理 5.1**　假定 $2\nmid h, 2|k; h'$ 为适合 $hh'\equiv 1(\bmod k)$ 的一个正整数; $\omega_{h,k}$ 由 §2 所定义, 及

$$x = \exp\left(-\frac{2\pi z}{k}+\frac{2h\pi\mathrm{i}}{k}\right),\quad x' = \exp\left(-\frac{2\pi}{kz}-\frac{2h'\pi\mathrm{i}}{k}\right),$$

此处 $z$ 的实数部分为正的, 则

$$f(x) = \omega_{h,k}\exp\left(-\frac{\pi}{12kz}+\frac{\pi z}{12k}\right)f(x').$$

**证明**　若我们取 $a=h, b=-k, c=(1-hh')/k, d=h'$, 则 $ad-bc=1$. 记

$$x = q^2 = \mathrm{e}^{2\pi\mathrm{i}\tau},\quad x' = Q^2 = \mathrm{e}^{2\pi\mathrm{i}T},$$

$$\tau = (h+\mathrm{i}z)/k,\quad T = (-h'+\mathrm{i}/z)/k,$$

则我们易于验证

$$T=\frac{c+d\tau}{a+b\tau}.$$

同 Tannery 与 Molk 的记号得

$$f(x)=\frac{1}{2^{1/3}}q^{-1/12}\frac{\phi(\tau)}{\chi(\tau)},\quad f(x')=\frac{1}{2^{1/3}}Q^{-1/12}\frac{\phi(T)}{\chi(T)}.$$

所以

$$\begin{aligned}f(x')&=\frac{1}{2^{1/3}}Q^{-1/12}\frac{\phi(T)}{\chi(T)}\\&=\exp\Big(\pi\mathrm{i}\Big(\frac{1}{8}(d^2-1)(c-1)+\frac{cd}{8}\\&\quad-\frac{(b-c)(bcd-a)}{24}\Big)\Big)\frac{1}{2^{1/3}}Q^{-1/12}\frac{\phi(\tau)}{\chi(\tau)}\\&=\exp\Big(\pi\mathrm{i}\Big(\frac{1}{8}(d^2-1)(c-1)+\frac{cd}{8}-\frac{(b-c)(bcd-a)}{24}\Big)\Big)\\&\quad\cdot q^{1/12}Q^{-1/12}f(x)\\&=\exp\Big(\pi\mathrm{i}\Big(\frac{1}{8}(d^2-1)(c-1)+\frac{cd}{8}-\frac{(b-c)(bcd-a)}{24}\Big)\Big)\\&\quad\cdot\exp\Big(\frac{\pi}{12k}\Big(\frac{1}{z}-z\Big)\Big)\exp\Big(\frac{\pi\mathrm{i}}{12k}(h+h')\Big)f(x).\end{aligned}$$

**引理 5.2** 假定 $2\nmid hk, hh'\equiv 1(\mathrm{mod}2k)$, 及

$$f_1(x)=\prod_1^{\infty}(1+x^{n-1/2})=1+\sum_{n=1}^{\infty}q_1(n)x^{n/2}.$$

则

$$f(x)=\frac{\omega_{h,k}}{2^{1/2}}\exp\left(\frac{\pi}{12k}\left(z+\frac{1}{2z}\right)\right)f_1(x').$$

**证明** 如引理 5.1, 我们有

$$\begin{aligned}f_1(x)&=f_1(q^2)=\prod(1+q^{2n-1})=2^{1/6}q^{1/24}\frac{1}{\chi(\tau)},\\f_1(x')&=2^{1/6}Q^{1/24}\frac{1}{\chi(T)}\\&=2^{1/6}Q^{1/24}\exp\left(-\frac{(b-c)(abc-d)}{24}\pi\mathrm{i}\right)\frac{\phi(\tau)}{\chi(\tau)}\\&=2^{1/6}Q^{1/24}\exp\left(-\frac{(b-c)(abc-d)}{24}\pi\mathrm{i}\right)2^{1/3}q^{1/12}f(x)\\&=\exp\left(-\frac{(b-c)(abc-d)}{24}\pi\mathrm{i}\right)2^{1/2}\end{aligned}$$

$$\cdot \exp\left(\frac{\pi \mathrm{i}}{24}\left(-\frac{h'}{k}+\frac{\mathrm{i}}{kz}+\frac{2h}{k}+\frac{2\mathrm{i}z}{k}\right)\right)f(x).$$

**引理 5.3** 假定 $2|h, 2\nmid k, hh'\equiv 1(\mathrm{mod}k), 2|h'$, 及

$$f_2(x)=\prod_1^{\infty}(1-x^{n-1/2})=1+\sum q_2(n)x^{n/2}.$$

则

$$f(x)=\frac{\omega_{h,k}}{2^{1/2}}\exp\left(\frac{\pi}{12k}\left(z+\frac{1}{2z}\right)\right)f_2(x').$$

**证明** 取

$$a=-h,\quad b=k,\quad c=(hh'-1)/k,\quad d=-h',$$

则

$$\begin{aligned}f_2(x')&=f_2(Q^2)=2^{1/6}Q^{1/24}\frac{\Psi(T)}{\chi(T)}\\&=2^{1/6}Q^{1/24}\exp\left(\frac{\pi \mathrm{i}}{2}\left(\frac{b^2-1}{4}+\frac{ab}{4}-\frac{(a+d)(abd-c)}{12}\right)\right)\cdot\frac{\phi(\tau)}{\chi(\tau)}\\&=2^{1/2}\exp\left(\frac{\pi \mathrm{i}}{2}\left(\frac{b^2-1}{4}+\frac{ab}{4}-\frac{(a+d)(abd-c)}{12}\right)\right)\cdot Q^{1/24}q^{1/12}f(x).\end{aligned}$$

## 6. 被积函数的逼近

命

$$z=k(N^{-2}-\mathrm{i}\vartheta).$$

则

$$\begin{aligned}I_1&=\sum_{1\leqslant k\leqslant N,\ 2|k}\ \sum_{(h,k)=1,0<h<k}\int_{-k^{-1}(N+1)^{-1}}^{k^{-1}(N+1)^{-1}}g(\vartheta)f(\mathrm{e}^{(2\pi \mathrm{i}h-2\pi z)/k})\mathrm{e}^{-2\pi \mathrm{i}hn/k+2\pi zn/k}\mathrm{d}\vartheta\\&=\sum_{1\leqslant k\leqslant N,2|k}\ \sum_{(h,k)=1,0<h<k}\int_{-k^{-1}(N+1)^{-1}}^{k^{-1}(N+1)^{-1}}g(\vartheta)\omega_{h,k}\mathrm{e}^{(\pi/12k)(z-1/z)}\\&\quad\cdot f(x')\mathrm{e}^{-2\pi \mathrm{i}hn/k+2\pi zn/k}\mathrm{d}\vartheta\\&=\sum_{1\leqslant k\leqslant N,2|k}\ \sum_{(h,k)=1,0<h<k}\int_{-k^{-1}(N+1)^{-1}}^{k^{-1}(N+1)^{-1}}g(\vartheta)\omega_{h,k}\\&\quad\cdot \mathrm{e}^{(\pi/12k)(z-1/z)-2\pi \mathrm{i}hn/k+2\pi zn/k}\sum_{\nu=0}^{\infty}q(\nu)\mathrm{e}^{-(2\pi/kz+2h'\pi \mathrm{i}/k)\nu}\mathrm{d}\vartheta\end{aligned}$$

$$= \sum_{1\leqslant k\leqslant N,2|k}\ \sum_{(h,k)=1,0<h<k} \int_{-k^{-1}(N+1)^{-1}}^{k^{-1}(N+1)^{-1}} \sum_{\nu=0}^{\infty} q(\nu)\mathrm{e}^{-(2\pi/kz)(\nu+1/24)+(2\pi z/k)(n+1/24)}$$
$$\cdot \sum_{r=1}^{k} b_r \mathrm{e}^{2\pi\mathrm{i}rh'/k}\omega_{h,k}\mathrm{e}^{-2\pi\mathrm{i}hn/k-2\pi\mathrm{i}h'\nu/k}\mathrm{d}\vartheta. \tag{6.1}$$

由于 $(1/k)R(1/z) \geqq \frac{1}{2}$, 所以

$$|I_1| \leqq \sum_{1\leqslant k\leqslant N,2|k} \int_{-k^{-1}(N+1)^{-1}}^{k^{-1}(N+1)^{-1}} \sum_{\nu=0}^{\infty} q(\nu)$$
$$\cdot \exp\left\{-\frac{2\pi}{k}\left(\nu+\frac{1}{24}\right)R\frac{1}{z}+\frac{2\pi}{k}\left(n+\frac{1}{24}\right)Rz\right\}$$
$$\sum_{r=1}^{k}|b_r|\left|\sum_{(h,k)=1}\omega_{h,k}\mathrm{e}^{-2\pi\mathrm{i}hn/k+2h'(r-\nu)\pi\mathrm{i}/k}\right|d\vartheta$$
$$= O\left(\sum_{k=1}^{N}\int_{-k^{-1}(N+1)^{-1}}^{k^{-1}(N+1)^{-1}}\sum_{\nu=0}^{\infty}q(\nu)\mathrm{e}^{-\pi(\nu+1/24)}\sum_{r=1}^{k}|b_r|k^{2/3}\mathrm{d}\vartheta\right)$$
$$= O\left(\sum_{k=1}^{N}\log k\cdot k^{2/3}\frac{1}{kN}\right) = O\left(\frac{1}{N}\sum_{k=1}^{N}k^{-1/3+\varepsilon}\right)$$
$$= O(N^{-1/3+\varepsilon}).$$

命

$$J = \frac{1}{2^{1/2}}\sum_{k=1,k\ \mathrm{odd}}^{N}\ \sum_{(h,k)=1,0<h\leqq k}\int_{-k^{-1}(N+1)^{-1}}^{k^{-1}(N+1)^{-1}} g(\vartheta)\omega_{h,k}$$
$$\cdot \mathrm{e}^{(\pi/24k)(2z+1/z)-2\pi\mathrm{i}hn/k+2\pi zn/k}\mathrm{d}\vartheta.$$

用同样的方法得 $|I_2 - J| = O(N^{-1/3+\varepsilon})$.

## 7. 一个围道积分

命 $\omega = N^{-2}-\mathrm{i}\vartheta$, 则

$$J = \frac{-\mathrm{i}}{2^{1/2}}\sum_{1\leqslant k\leqslant N,k\ \mathrm{odd}}\ \sum_{(h,k)=1,0<h\leqslant k}\omega_{h,k}\mathrm{e}^{-2\pi\mathrm{i}hn/k}$$
$$\cdot\int_{N^{-2}-\mathrm{i}\vartheta_2}^{N^{-2}+\mathrm{i}\vartheta_1}\mathrm{e}^{2\pi\omega(n+1/24)+\pi/24k^2\omega}\mathrm{d}\omega$$

$$
\begin{aligned}
&= \frac{\mathrm{i}}{2^{1/2}} \sum_{1\leqslant k\leqslant N, k\ \mathrm{odd}} \sum_{(h,k)=1, 0<h\leqslant k} \omega_{h,k} \mathrm{e}^{-2\pi \mathrm{i} hn/k} \\
&\quad \cdot \Big( \int_{N^{-2}+\mathrm{i}\vartheta_1}^{N^{-2}+\mathrm{i}k^{-1}(N+1)^{-1}} + \int_{N^{-2}+\mathrm{i}k^{-1}(N+1)^{-1}}^{-N^{-2}+\mathrm{i}k^{-1}(N+1)^{-1}} + \int_{-N^{-2}+\mathrm{i}k^{-1}(N+1)^{-1}}^{-N^{-2}-\mathrm{i}k^{-1}(N+1)^{-1}} \\
&\quad + \int_{-N^{-2}-\mathrm{i}k^{-1}(N+1)^{-1}}^{N^{-2}+\mathrm{i}k^{-1}(N+1)^{-1}} + \int_{N^{-2}-\mathrm{i}k^{-1}(N+1)}^{N^{-2}-\mathrm{i}\vartheta_2} - 2\pi \mathrm{i}\mathrm{Residue\ at\ } 0 \Big) \\
&= K_1 + K_2 + K_3 + K_4 + K_5 + L(\text{定义}),
\end{aligned}
$$

$$
\begin{aligned}
K_1 = \frac{\mathrm{i}}{2^{1/2}} &\sum_{1\leqslant k\leqslant N, k\ \mathrm{odd}} \sum_{(h,k)=1, 0<h\leqslant k} \omega_{h,k} \mathrm{e}^{-2\pi \mathrm{i} hn/k} \\
&\cdot \int_{N^{-2}+\mathrm{i}k^{-1}(N+k)^{-1}}^{N^{-2}+\mathrm{i}k^{-1}(N+1)^{-1}} g(\vartheta) \mathrm{e}^{2\pi\omega(n+1/24)+\pi/24k^2\omega} \mathrm{d}\omega.
\end{aligned}
$$

由引理 3.1 得

$$
\begin{aligned}
K_1 &= O\Big( \sum_{1\leqslant k\leqslant N, K\mathrm{odd}} k^{2/3+\varepsilon} \int_{k^{-1}(N+k)^{-1}}^{k^{-1}(N+1)^{-1}} \exp\left\{ 2\pi \left( n + \frac{1}{24} \right) R\omega + \frac{\pi}{24k^2} R\frac{1}{\omega} \right\} \mathrm{d}\omega \\
&= O\left( \sum_{k=1}^{N} k^{2/3+\varepsilon} \mathrm{e}^{-2\pi n N^{-2}} \int_{k^{-1}(N+k)^{-1}}^{k^{-1}(N+1)^{-1}} \mathrm{d}\vartheta \right) \\
&= O(N^{-1/3+\varepsilon}).
\end{aligned}
$$

关于 $K_5$, 类似的结果成立.

我们有

$$
R\frac{1}{k^2\omega} = \frac{N^{-2}}{k^2 N^{-2} + N^2}, \quad K_2 = O\left( \sum_{k=1}^{N} N^{-2} k^{2/3+\varepsilon} \right) = O(N^{-1/3+\varepsilon}).
$$

关于 $K_4$, 类似的结果成立.

再将 Kloosterman 的论证用于 $K_3$, 得 $K_3 = O(N^{-1/3})$.

最后我们来寻求 $\exp(2\pi\omega(n+1/24)+\pi/24k^2\omega)$ 在 $\omega=0$ 处的残数, 我们有展开式

$$
\mathrm{e}^{2\pi\omega(n+1/24)} = \sum_{\nu=1}^{\infty} \frac{(2\pi\omega(n+1/24))^\nu}{\nu!},
$$

$$
\mathrm{e}^{\pi/24k^2\omega} = \sum_{\mu=1}^{\infty} \frac{1}{\mu!} \left( \frac{\pi}{24k^2\omega} \right)^\mu.
$$

所以残数为

$$
\sum_{\mu=1}^{\infty} \frac{1}{\mu!} \left( \frac{\pi}{24k^2} \right)^\mu \frac{1}{(\mu-1)!} \left( 2\pi \left( n + \frac{1}{24} \right) \right)^{\mu-1}
$$

$$= \frac{1}{2\pi}\frac{\mathrm{d}}{\mathrm{d}n}\sum_{\mu=1}^{\infty}\frac{1}{(\mu!)^2}\left(\frac{\pi}{24k^2}\right)^{\mu}\left(2\pi\left(n+\frac{1}{24}\right)\right)^{\mu}$$

$$= \frac{1}{2\pi}\frac{\mathrm{d}}{\mathrm{d}n}\sum_{\mu=1}^{\infty}\frac{1}{2^{2\mu}(\mu!)^2}\left(\frac{\pi}{k}\left\{\frac{1}{3}\left(n+\frac{1}{24}\right)\right\}^{1/2}\right)^{2\mu}$$

$$= \frac{1}{2\pi}\frac{\mathrm{d}}{\mathrm{d}n}J_0\left(\frac{\mathrm{i}\pi}{k}\left\{\frac{1}{3}\left(n+\frac{1}{24}\right)\right\}^{1/2}\right).$$

因此

$$q(n) = \frac{1}{2^{1/2}}\sum_{k=1,k \text{ odd}}^{N}\sum_{(n,k)=1,0<h\leqslant k}\omega_{h,k}\mathrm{e}^{-2\pi\mathrm{i}hn/k}\frac{\mathrm{d}}{\mathrm{d}n}J_0$$

$$\cdot\left(\frac{\mathrm{i}\pi}{k}\left\{\frac{1}{3}\left(n+\frac{1}{24}\right)\right\}^{1/2}\right) + O(N^{-1/3+\varepsilon}).$$

当 $N\to\infty$ 即得定理.

(王元　译)

# 关于 Pell 氏方程的最小解①

华罗庚 (国立清华大学)

命 $x_0, y_0$ 为 Pell 氏方程

$$x^2 - dy^2 = 4$$

的最小正解, 此处 $d$ 为一个正整数, 它不是一个完全平方, 而且同余于 0 或 1(mod 4). 命 $\varepsilon = (x_0 + d^{1/2}y_0)/2$, 则 Schur②曾证明过

$$\varepsilon < d^{d^{1/2}} \tag{1}$$

或更确切地

$$\log \varepsilon < d^{1/2}((1/2)\log d + (1/2)\log\log d + 1). \tag{2}$$

当 $d > 244.69$ 时, 他利用性质

$$d^{1/2}((1/2)\log d + (1/2)\log\log d + 1) < d^{1/2}\log d$$

将 (1) 由 (2) 导出. 而当 $d \leqslant 244$ 时, (1) 式可以由直接计算得出. 本文的目的为证明一个稍好的结果

$$\log \varepsilon < d^{1/2}((1/2)\log d + 1). \tag{3}$$

由此不需要作任何计算即得 (1), 本文所用的方法为以前论文所述的方法.

命 $(d/r)$ 为 Kronecker 符号 (当 $r_1 \equiv r_2 \pmod d$ 时, 定义 $(d|r_1) = (d|r_2)$. 这样我们就将定义延拓至负整数 $r$).

命 $f$ 表示与 $d$ 有关的基本判别式, 即

$$d = m^2 f,$$

此处 $f$ 不能被一个奇素数的平方整除, 及它或者为一个奇数或者同余于 8 或 12 (mod 16).

**引理 1** 当 $d > 0$ 时有

$$\left(\frac{d}{r}\right) = \left(\frac{d}{-r}\right).$$

---

① 1941 年 12 月 3 日收到. 发表于*Bull. Amer. Math. Soc.*, 1942, 48: 731-735.

② *Göttingen Nechrichter*, 1918: 30-36.

**证明** 见 Landace. *Vorlesungen über Zahlentheorie*, Vol. 1, Theorem 101.

**引理 2** 我们有

$$\sum_r \left(\frac{f}{r}\right) \mathrm{e}^{2\pi i n r/f} = \left(\frac{f}{n}\right) f^{1/2},$$

此处 $r$ 过 mod $f$ 的一个完全剩余系.

**证明** 见上面引述的 Landace 著作, 定理 215.

**引理 3** 我们有

$$\frac{1}{A^*+1}\left|\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{f}{n}\right)\right| \leqslant \frac{1}{2}\left(f^{1/2} - \frac{A^*+1}{f^{1/2}}\right),$$

此处 $A^*$ 表示 $A \bmod f$ 的最小正剩余.

**证明**(见前文之引理 1) 由引理 2 可知

$$\begin{aligned} f^{1/2}\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{f}{n}\right) &= \frac{1}{2}f^{1/2}\sum_{a=0}^{A}\sum_{n=-a}^{a}\left(\frac{f}{n}\right) \\ &= \frac{1}{2}\sum_{a=0}^{A}\sum_{n=-a}^{a}\sum_{r=1}^{f}\left(\frac{f}{r}\right)\mathrm{e}^{2\pi i n r/f} \\ &= \frac{1}{2}\sum_{r=1}^{f}\left(\frac{f}{r}\right)\sum_{a=0}^{A}\sum_{n=-a}^{a}\mathrm{e}^{2\pi i n r/f}. \end{aligned}$$

由于

$$\sum_{r=1}^{f-1}\mathrm{e}^{2\pi i n r/f} = \sum_{r=1}^{f}\mathrm{e}^{2\pi i n r/f} - 1 = \begin{cases} -1, & 当\ f\nmid n, \\ f-1, & 当\ f\mid n. \end{cases}$$

所以

$$\begin{aligned} f^{1/2}\left|\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{f}{n}\right)\right| &\leqq \frac{1}{2}\sum_{r=1}^{f-1}\left|\sum_{a=0}^{A}\sum_{n=-a}^{a}\mathrm{e}^{2\pi i n r/f}\right| \\ &= \frac{1}{2}\sum_{r=1}^{f-1}\left(\frac{\sin(A+1)\pi r/f}{\sin \pi r/f}\right)^2 \\ &= \frac{1}{2}\sum_{r=1}^{f-1}\left(\frac{\sin(A^*+1)\pi r/f}{\sin \pi r/f}\right)^2 \\ &= \frac{1}{2}\sum_{r=1}^{f-1}\sum_{a=0}^{A*}\sum_{n=-a}^{a}\mathrm{e}^{2\pi i n r/f} \\ &= \frac{1}{2}((A^*+1)f - (A^*+1)^2). \end{aligned}$$

**引理 4**　对于任何判别式 $d>0$ 及 $A>d^{1/2}$, 我们有

$$\left|\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{d}{n}\right)\right| \leqslant \frac{1}{2}Ad^{1/2}.$$

**证明**　熟知①

$$\left(\frac{d}{n}\right)=\left(\frac{f}{n}\right)\sum_{r|(m,n)}\mu(r).$$

所以

$$\begin{aligned}\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{d}{n}\right)&=\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{f}{n}\right)\sum_{r|(m,n)}\mu(r)\\&=\sum_{r|m}\mu(r)\sum_{a=1}^{A}\sum_{n=1,r|n}^{a}\left(\frac{f}{n}\right)\\&=\sum_{r|m}\mu(r)\sum_{a=1}^{A}\sum_{n=1}^{[a/r]}\left(\frac{f}{rn}\right)\\&=\sum_{r|m}\mu(r)\left(\frac{f}{r}\right)\sum_{a=1}^{A}\sum_{n=1}^{[a/r]}\left(\frac{f}{n}\right).\end{aligned}$$

由于我们有 $f^{1/2}r<f^{1/2}m<A$,

$$f^{1/2}-\frac{1}{f^{1/2}}\left(\left[\frac{A}{r}\right]+1\right)^2<f^{1/2}-\frac{1}{f^{1/2}}\cdot f=0$$

与

$$\sum_{r|m}1\leqq m,$$

因此由引理 2 得

$$\begin{aligned}\left|\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{d}{n}\right)\right|&\leqslant\frac{1}{2}\sum_{r|m}\left|\sum_{a=1}^{A}\sum_{n=1}^{[a/r]}\left(\frac{f}{n}\right)\right|\\&\leqslant\frac{1}{2}\sum_{r|m}r\left|\sum_{b=1}^{[A/r]}\sum_{n=1}^{b}\left(\frac{f}{n}\right)\right|\\&\leqslant\frac{1}{2}\sum_{r|m}r\left(\left(\left[\frac{A}{r}\right]+1\right)f^{1/2}-\frac{1}{f^{1/2}}\left(\left[\frac{A}{r}\right]+1\right)^2\right)\end{aligned}$$

① 这可以由下面的事实推出, 即当 $a>1$ 或 $a=1$ 时有 $\sum_{d|a}\mu(d)=0$ 或 1.

$$\leqslant \frac{1}{2}\sum_{r|m} r\cdot\frac{A}{r}f^{1/2} \leqslant \frac{1}{2}Af^{1/2}m = \frac{1}{2}Ad^{1/2}.$$

**引理 5** 我们有

$$\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{1}{n} < \frac{1}{2}\log d + 1.$$

**证明** 当 $n \geqq 1$ 时, 命

$$S(n) = \sum_{a=1}^{n}\sum_{m=1}^{a}\left(\frac{d}{m}\right),$$

及命 $S(0) = S(-1) = 0$. 则

$$S(n) - 2S(n-1) + S(n-2) = \left(\frac{d}{n}\right), \quad n \geqq 1$$

与

$$\begin{aligned}\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{1}{n} &= \sum_{n=1}^{\infty}\{S(n) - 2S(n-1) + S(n-2)\}\frac{1}{n}\\ &= \sum_{n=1}^{\infty} S(n)\left(\frac{1}{n} - \frac{2}{n+1} + \frac{1}{n+2}\right)\\ &= \sum_{n=1}^{\infty}\frac{2S(n)}{n(n+1)(n+2)}.\end{aligned}$$

我们将这一级数分成两部分

$$S_1 = \sum_{n=1}^{A-1}, \quad S_2 = \sum_{n=A}^{\infty}.$$

由于

$$|S(n)| \leqslant \sum_{a=1}^{n}\sum_{m=1}^{a} 1 = \frac{n(n+1)}{2},$$

所以

$$|S_1| \leqq \sum_{n=1}^{A-1}\frac{1}{n+2}.$$

若 $A > d^{1/2}$, 则由引理 4 得

$$|S_2| < \sum_{n=A}^{\infty}\frac{nd^{1/2}}{n(n+1)(n+2)} = \frac{d^{1/2}}{A+1}.$$

所以

$$\left|\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{1}{n}\right| \leqslant \sum_{n=1}^{A-1}\frac{1}{n+2}+\frac{d^{1/2}}{A+1}$$
$$=\sum_{m=1}^{A-1}\frac{1}{m}-1-\frac{1}{2}+\frac{1}{A}+\frac{1}{A+1}+\frac{d^{1/2}}{A+1}$$
$$\leqslant \log(A-1)-\frac{1}{2}+\frac{1}{A}+\frac{d^{1/2}+1}{A+1}.$$

取 $A=[d^{1/2}]+1$, 由于 $d \geqslant 5$, 所以

$$\left|\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{1}{n}\right| \leqslant \log d^{1/2}-\frac{1}{2}+\frac{1}{d^{1/2}}+\frac{d^{1/2}+1}{d^{1/2}+1}$$
$$=\frac{1}{2}\log d+\frac{1}{2}+\frac{1}{d^{1/2}}<\frac{1}{2}\log d+1.$$

**定理 1** 我们有

$$\log\varepsilon < d^{1/2}((1/2)\log d+1).$$

**证明** 熟知具有判别式 $d>0$ 的非等价二次型类的类数 $h(d)$ 等于

$$h(d)=\frac{d^{1/2}}{\log\varepsilon}\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{1}{n}.$$

由于 $h(d) \geqq 1$, 故得定理

**定理 2**(Schur) 我们有

$$\log\varepsilon \leqslant d^{1/2}\log d.$$

**证明** 当 $d>\mathrm{e}^2$ 时, 由定理 1 即得定理. 若 $d<\mathrm{e}^2$, 则 $d=5$. 显然 $\varepsilon=(3+5^{1/2})/2$ 及

$$\log\varepsilon < 5^{1/2}\log 5.$$

(王元 译)

# 关于素数的最小原根①

华罗庚 (国立清华大学)

Vinogradov②证明了, 素数 $p$ 的最小正原根 $g(p)$ 为 $O(2^m p^{\frac{1}{2}}\log p)$, 这里 $m$ 表示 $p-1$ 的不同素因子的个数. 1930 年, 他③将此结果改进为

$$g(p)=O(2^m p^{\frac{1}{2}}\log\log p),$$

或更准确地,

$$g(p)\leqslant 2^m\frac{p-1}{\phi(p-1)}p^{\frac{1}{2}}.$$

本文的目的是要通过引入特征和平均值的概念④ 来证明: 如果 $h(p)$ 表示有最小绝对值的原根 mod $p$, 则有

$$|h(p)|<2^m p^{\frac{1}{2}};$$

当 $p\equiv 1(\text{mod}4)$ 时, 我们有

$$g(p)<2^m p^{\frac{1}{2}},$$

而当 $p\equiv 3(\text{mod}4)$ 时, 则有

$$g(p)<2^{m+1}p^{\frac{1}{2}}.$$

因为

$$\frac{p-1}{\phi(p-1)}\geqslant 2,$$

所以, 我们的结果总比 Vinogradov 的要好.

**引理 1** 设 $p>2, 1\leqslant A<p$. 则对于每一个非主特征⑤$\chi(n)\text{mod}p$, 我们有

$$\frac{1}{A+1}\left|\sum_{a=0}^{A}\sum_{n=-a}^{a}\chi(n)\right|\leqslant p^{\frac{1}{2}}-\frac{A+1}{p^{\frac{1}{2}}}.$$

---

① 1941 年 12 月 3 日收到. 发表于*Bull. Amer. Math. Soc.*, 1942, 48: 726–730.

② 可见 Landau. *Vorlesungen über Zahlentheorie*, v.2, part 7, 第 14 章. Vinogradov 的原文在中国找不到.

③ *Comptes Rendus de l'Académie des Sciences de l'URSS*, 1930: 7–11.

④ 本文可以看作是某种方法的导引, 这种方法有着诸多的应用.

⑤ 可参见 Landau. *Vorlesungen über Zahlentheorie*, 1: 83–87.

**证明** 设 $\varepsilon = \mathrm{e}^{\frac{2\pi\mathrm{i}}{p}}$ 和

$$\tau(\chi) = \sum_{h=1}^{p-1} \chi(h)\varepsilon^h.$$

已知有

$$|\tau(\chi)| = p^{\frac{1}{2}}.$$

对于 $p \nmid n$, 我们有

$$\begin{aligned}\sum_{h=1}^{p-1} \overline{\chi}(h)\varepsilon^{hn} &= \chi(n) \sum_{h=1}^{p-1} \overline{\chi}(hn)\varepsilon^{hn} \\ &= \chi(n) \sum_{h=1}^{p-1} \overline{\chi}(h)\varepsilon^{h} = \chi(n)\tau(\bar{\chi}).\end{aligned}$$

当 $p|n$ 时, 因为 $\chi(n) = 0$ 和

$$\sum_{h=1}^{p-1} \overline{\chi}(h) = 0,$$

所以, 上述公式也成立. 因此

$$\begin{aligned}\tau(\overline{\chi}) \sum_{a=0}^{A} \sum_{n=-a}^{a} \chi(n) &= \sum_{h=1}^{p-1} \overline{\chi}(h) \sum_{a=0}^{A} \sum_{n=-a}^{a} \varepsilon^{hn} \\ &= \sum_{h=1}^{p-1} \overline{\chi}(h) \left( \frac{\sin(A+1)\frac{\pi h}{p}}{\sin \frac{\pi h}{p}} \right)^2.\end{aligned}$$

从而有

$$\begin{aligned}p^{\frac{1}{2}} \left| \sum_{a=0}^{A} \sum_{n=-a}^{a} \chi(n) \right| &\leqslant \sum_{h=1}^{p-1} \left( \frac{\sin(A+1)\frac{\pi h}{p}}{\sin \frac{\pi h}{p}} \right)^2 \\ &= \sum_{h=1}^{p-1} \sum_{a=0}^{A} \sum_{n=-a}^{a} \varepsilon^{hn} \\ &= \sum_{a=0}^{A} \sum_{n=-a}^{a} \left( \sum_{h=1}^{p} \varepsilon^{hn} - 1 \right) \\ &= (A+1)p - (A+1)^2.\end{aligned}$$

**引理 2** 设 $p>2, 1\leqslant A<\frac{p-1}{2}$. 则对于每一个非主特征 $\chi(n) \bmod p$, 我们有

$$\frac{1}{A+1}\left|\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}\chi(n)\right|\leqslant p^{\frac{1}{2}}-\frac{A+1}{p^{\frac{1}{2}}}.$$

**证明** 如同在引理 1 中一样, 我们有

$$\begin{aligned}&p^{\frac{1}{2}}\left|\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}\chi(n)\right|\\&=\left|\sum_{h=1}^{p-1}\overline{\chi}(h)\mathrm{e}^{2\pi\mathrm{i}h(A+1)/p}\left(\frac{\sin(A+1)\frac{\pi h}{p}}{\sin\frac{\pi h}{p}}\right)^2\right|\\&\leqslant\sum_{h=1}^{p-1}\left(\frac{\sin(A+1)\frac{\pi h}{p}}{\sin\frac{\pi h}{p}}\right)^2\\&=(A+1)p-(A+1)^2.\end{aligned}$$

**引理 3** 设 $p>2$. 如果 $n$ 不是一个原根 $\bmod p$, 则

$$\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{\chi^{(k)}}\chi^{(k)}(n)=0,$$

其中 $\chi^{(k)}$ 过所有这样的特征, 它们满足条件: $k$ 是最小的正整数, 使得 $(\chi)^k$ 为主特征 (参见 139 页的脚注⑤ 496 页. 那里的条件 $1\leqslant n<p$ 是不必要的).

**定理 1** 我们有

$$|h(p)|<2^m p^{\frac{1}{2}}.$$

**证明** 设 $p>2$. 由引理 3 可得,

$$0=\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{\chi^{(k)}}\sum_{a=0}^{|h(p)|-1}\sum_{n=-a}^{a}\chi^{(k)}(n).$$

对于 $k=1$, 右端给出

$$\sum_{a=0}^{|h(p)|-1}\sum_{n=-a}^{a}\chi^{(1)}(n)=\sum_{a=0}^{|h(p)|-1}2a=|h(p)|^2-|h(p)|.$$

另一方面, 对于 $k\neq 1$, 由引理 1(取 $A=|h(p)|-1$) 可得

$$\left|\sum_{a=0}^{|h(p)|-1}\sum_{n=-a}^{a}\chi^{(k)}(n)\right|\leqslant |h(p)|p^{\frac{1}{2}}-\frac{|h(p)|^2}{p^{\frac{1}{2}}}.$$

因此

$$|h(p)|^2-|h(p)|\leqslant\left(|h(p)|p^{\frac{1}{2}}-\frac{|h(p)|^2}{p^{\frac{1}{2}}}\right)\sum_{k|p-1}\frac{|\mu(k)|}{\phi(k)}\phi(k)$$
$$=2^m\left(|h(p)|p^{\frac{1}{2}}-\frac{|h(p)^2|}{p^{\frac{1}{2}}}\right).$$

从而有

$$|h(p)|\leqslant\frac{2^mp^{\frac{1}{2}}+1}{1+2^mp^{-\frac{1}{2}}}<2^mp^{\frac{1}{2}}.$$

**推论**　对于 $p\equiv 1(\bmod 4)$, 我们有

$$g(p)=|h(p)|<2^mp^{\frac{1}{2}}.$$

**证明**　我们需要证明 $|h(p)|$ 是一个原根. 如若不然, 则 $-|h(p)|$ 是原根, 而 $|h(p)|$ 属于一个指数 $l$, 这里 $l|(p-1), l<p-1$. 即

$$|h(p)|^l\equiv 1(\bmod\ p),\quad (h(p))^{2l}\equiv 1(\bmod\ p).$$

从而有 $2l=p-1$ 和 $|h(p)|^{\frac{p-1}{2}}\equiv 1(\bmod p)$. 因此, $|h(p)|$ 是一个二次剩余. 因为 $-1$ 是一个二次剩余 mod $p$, 所以, $-|h(p)|$ 也是一个二次剩余, 且有 $(-|h(p)|)^{\frac{p-1}{2}}\equiv 1(\bmod p)$. 但这与 $-|h(p)|$ 是原根相矛盾.

**注**　有时候, 定理 1 可以用

$$\sum_{n=-a}^{a}\chi^{(k)}(n)=0$$

来改进, 而这可以由 $\chi^{(k)}(-1)=-1$(可推出 $\chi^{(k)}(n)=-\chi^{(k)}(-n)$) 来得到. 因而, 对于 $p\equiv 3(\bmod\ 4)$, 有

$$|h(p)|<2^{m-1}p^{\frac{1}{2}}.$$

事实上, 我们有 $g^{\frac{p-1}{2}}\equiv -1(\bmod\ p)$ 和 $\chi^{(k)}(g)=\mathrm{e}^{\frac{2\pi i\lambda}{k}}$. 因为

$$-1=\chi^{(k)}(g^{\frac{p-1}{2}})=\mathrm{e}^{\frac{\pi i(p-1)\lambda}{k}},$$

所以, 我们有 $2\nmid\frac{(p-1)\lambda}{k}$. 引理 3 公式中的项都是关于无平方因子数 $k$ 的. 因此, $\chi^{(k)}(-1)=-1$ 仅对 $p\equiv 3(\bmod\ 4)$ 和 $2\nmid\lambda$ 成立. 我们可见, 当 $2|k$ 时, 有

$$\sum_{a=0}^{|h(p)|-1}\sum_{n=-a}^{a}\chi^{(k)}(n)=0.$$

从而有

$$|h(p)|^2-|h(p)|\leqslant\left(|h(p)|p^{\frac{1}{2}}-\frac{|h(p)|^2}{p^{\frac{1}{2}}}\right)\sum_{k\left|\frac{p-1}{2}\right.}|\mu(k)|$$

$$=2^{m-1}\left(|h(p)|p^{\frac{1}{2}}-\frac{|h(p)|^2}{p^{\frac{1}{2}}}\right).$$

因此, 我们可得

$$|h(p)|\leqslant\frac{2^{m-1}p^{\frac{1}{2}}+1}{1+2^{m-1}p^{-\frac{1}{2}}}<2^{m-1}p^{\frac{1}{2}}.$$

**定理 2** 我们有

$$g(p)<2^{m+1}p^{\frac{1}{2}}.$$

**证明** 设 $A$ 为不超过 $\frac{g-1}{2}$ 的最大整数, 则

$$0=\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{\chi^{(k)}}\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}\chi^{(k)}(n).$$

对于 $k=1$, 右端给出

$$\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}\chi^{(1)}(n)=\sum_{a=0}^{A}(2a+1)=(A+1)^2.$$

对于 $k\neq 1$, 我们有

$$\left|\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}\chi^{(k)}(n)\right|\leqslant(A+1)p^{\frac{1}{2}}-\frac{1}{p^{\frac{1}{2}}}(A+1)^2.$$

因此, 与定理 1 的证明中一样, 我们有

$$(A+1)^2<2^m\left((A+1)p^{\frac{1}{2}}-\frac{1}{p^{\frac{1}{2}}}(A+1)^2\right),$$

$$\frac{g-1}{2}<A+1\leqslant\frac{2^mp^{\frac{1}{2}}}{1+2^mp^{-\frac{1}{2}}},$$

即

$$g\leqslant\frac{2^{m-1}p^{\frac{1}{2}}}{1+2^mp^{-\frac{1}{2}}}+1<2^{m+1}p^{\frac{1}{2}}.$$

(贾朝华 译)

# 圆内格点①

华罗庚

命 $R(x)$ 表示圆 $u^2+v^2=x$ 内及其边界上的格点个数, 我们易于证明, 当 $x\to\infty$ 时, $R(x)\sim\pi x$, 及事实上, 存在某个小于 1 的正数 $\alpha$ 使

$$R(x)=\pi x+O(x^{\alpha}). \tag{1}$$

我们的问题在于寻求使 (1) 式成立的 $\alpha$ 的下界 $\theta$. 以往最好的估计为 $\theta\leqslant 15/46$, 这是 Titchmarsh②于 1933 年证明的. 本文的目的为证明 $\theta\leqslant 13/40$. Titchmarsh 的证明主要依赖于他所利用的一个二次型是定正的. 欲改进这一结果, 我们遇到的困难为某二次型不是定正的, 但经检验后, 我们发现二次型的变数不是完全一般的. 限制于这些变数, 我们幸运地得到型的值总是正的.

1. 征引自 Titchmarsh 文章中的引理

**引理 1** 命 $a_{\mu v}$ 为任意实数或复数满足: 若 $S_{m,n}=\sum\limits_{\mu=1}^{m}\sum\limits_{v=1}^{n}a_{\mu_1 v}$ 则 $|S_{m,n}|\leqslant G(1\leqslant m\leqslant M;1\leqslant n\leqslant N)$. 命 $b_{m,n}$ 表示实数, $0\leqslant b_{m,n}\leqslant H$, 及下面每一个表达式

$$b_{m,n}-b_{m,n+1},\quad b_{m,n}-b_{m+1,n},\quad b_{m,n}-b_{m+1,n}-b_{m,n+1}+b_{m+1,n+1}.$$

对于问题中的 $m$ 与 $n$ 皆同号, 则

$$\left|\sum_{m=1}^{M}\sum_{n=1}^{N}a_{m,n}b_{m,n}\right|\leqslant 5GH.$$

**引理 2** 命 $f(x,y)$ 为 $x$ 与 $y$ 的实函数, 及

$$S=\sum\sum \mathrm{e}^{2\pi\mathrm{i}f(m,n)},$$

---

① 1942 年 1 月 9 日收到. 发表于*Quart. J. Math. Oxford Ser.*, 1942, 13: 18–29.

② *Proc. London Math. Soc*(2)., 1935, 38: 96–115. 我必须提到 I. Vinogradov 的一篇文章, *Bull. Acad. Sci. V. R. S. S.*, 1932, 7: 313–316, 在该文中宣布了误差项为 $O(x^{17/53+\varepsilon})$. 但不幸的是在该证明中似乎有一个无法修补的错误. 即在该文的 §3 中的 $F$ 与 $G$. 他说, 经过复杂的计算, 得到估计 $\sum\limits_{n}\sum\limits_{n}\sum\min\{P,(E)^{-1}\}\min\{P,(F)^{-1}\}\leqslant P_1^4P_2^4P_3^4M^{2+\varepsilon}P^{-2}$. 但考虑具有 $r_1=s_1=0$ 之诸项之和即可知这是显然不对的 (实际上, 这些项构成的部分和 $\geqslant(M/P)^2P_1^2P_2^4P_3^4P^2$).

其中过矩形 $a \leqslant x \leqslant b, \alpha \leqslant y \leqslant \beta$ 中的一个区域 $D$ 中的格点求和. 命

$$S' = \sum\sum \mathrm{e}^{2\pi\mathrm{i}\{f(m+\mu,n+v)-f(m,n)\}},$$

$$S'' = \sum\sum \mathrm{e}^{2\pi\mathrm{i}\{f(m+\mu,n-v)-f(m,n)\}},$$

此处 $\mu$ 与 $v$ 为整数, 及 $S'$ 过使 $(m,n)$ 与 $(m+\mu,n+v)$ 皆属于 $D$ 之 $m$ 与 $n$ 求和; 类似地, $S''$ 亦然. 命 $\rho$ 为一个不超过 $b-a$ 的正整数, 及 $\rho'$ 为一个不超过 $\beta-\alpha$ 之正整数. 则

$$S = O\left\{\frac{(b-a)(\beta-\alpha)}{(\rho\rho')^{\frac{1}{2}}}\right\} + O\left[\left\{\frac{(b-a)(\beta-\alpha)}{\rho\rho'}\sum_{\mu=1}^{\rho-1}\sum_{v=0}^{\rho'-1}|S'|\right\}^{\frac{1}{2}}\right]$$
$$+ O\left[\left\{\frac{(b-a)(\beta-\alpha)}{\rho\rho'}\sum_{\mu=0}^{\rho-1}\sum_{v=1}^{\rho'-1}|S''|\right\}^{\frac{1}{2}}\right].$$

**引理 2′** 若 $0 < \rho \leqslant b-a$, 则

$$S = O\left\{\frac{(b-a)(\beta-\alpha)}{\rho^{\frac{1}{2}}}\right\} + O\left[\left\{\frac{(b-a)(\beta-\alpha)}{\rho}\sum_{\mu=1}^{\rho-1}|S'''|\right\}^{\frac{1}{2}}\right],$$

此处

$$S''' = \sum\sum \mathrm{e}^{2\pi\mathrm{i}\{f(m+\mu,n)-f(m,n)\}}.$$

**引理 3** 命 $f(x,y)$ 为 $x$ 与 $y$ 的可微实函数, 命对于所考虑的每一个 $y$ 值, $f_x(x,y)$ 为 $x$ 的单调函数, 及对于所考虑的每一个 $x$ 值, $f_y(x,y)$ 为 $y$ 的单调函数. 对于 $a \leqslant x \leqslant b, \alpha \leqslant y \leqslant \beta$, 命 $|f_x| \leqslant 3/4, |f_y| \leqslant 3/4$, 此处 $b-a \leqslant l, \beta-\alpha \leqslant l (l \geqslant 1)$. 命 $D$ 为矩形 $(a,b;\alpha,\beta)$, 或由连续单调曲线切割而成的该矩形的一部分. 则

$$\sum_D\sum \mathrm{e}^{2\pi\mathrm{i}f(m,n)} = \iint_D \mathrm{e}^{2\pi\mathrm{i}f(x,y)}\mathrm{d}x\mathrm{d}y + O(l). \tag{2}$$

**引理 4** 假定 $f(x,y)$ 为 $x$ 与 $y$ 的实函数, 它在矩形 $(a,b;\alpha,\beta)$ 中有所要求阶的连续偏微商, 及这些微商定义的给定次数的多项式等于 0 所定义的曲线与任何其他这类曲线或任何直线只有 $O(1)$ 个交点. 命 $b-a \leqslant l, \beta-\alpha \leqslant l$. 命在矩形 $(a,b;\alpha,\beta)$ 中,

$$|f_{xx}| < AR, \quad |f_{yy}| > AR, \quad |f_{xy}| < AR \tag{3}$$

($A$ 表示一个绝对正常数, 每次出现时不必要取同一值) 及

$$|f_{xx}f_{yy} - f_{xy}^2| \geqslant r^2, \tag{4}$$

此处 $0 < r < R$. 又命 $|f_x| \leqslant r_1, |f_y| \leqslant r_2, |f_{xxy}| \leqslant r_3, |f_{xyy}| \leqslant r_3, |f_{yyy}| \leqslant r_3$, 及

$$r_1 r_3 < K_1 r^2 \tag{5}$$

与

$$l r_3 < K_2 r, \tag{6}$$

此处 $K_1$ 与 $K_2$ 为充分小的常数, 则

$$\int_a^b \int_\alpha^\beta \mathrm{e}^{2\pi \mathrm{i} f(x,y)} \mathrm{d}x \mathrm{d}y = O\left(\frac{1 + |\log l| + |\log R|}{r}\right).$$

引理 1, 2, 3, 4 分别对应于 Titchmarsh 的引理 $\alpha, \beta, \gamma, \zeta$.

2. 命

$$\begin{aligned}\Delta f(u,v) =& f(u + m_1 + m_2 + m_3, v + n_1 + n_2 + n_3) \\ & - \sum f(u + m_1 + m_2, v + n_1 + n_2) \\ & + \sum f(u + m_1, v + n_1) - f(u,v),\end{aligned}$$

及命

$$X = 6m_1m_2m_3, \quad Y = 2\sum m_1m_2n_3,$$

$$Z = 2\sum m_1n_2n_3, \quad W = 6n_1n_2n_3.$$

则得

$$\Delta u = \Delta v = 0, \quad \Delta u^2 = \Delta uv = \Delta v^2 = 0,$$

$$\Delta u^3 = X, \quad \Delta u^2 v = Y, \quad \Delta uv^2 = Z, \quad \Delta v^3 = W.$$

若 $m_i = O(\eta)$ 及 $n_i = O(\eta)(i = 1,2,3)$, 则易于证明

$$\Delta(u^\lambda v^{k-1})_{u=0,v=0} = O\{\eta^{k-3}(|X| + |Y| + |Z| + |W|)\}.$$

命 $|u_1| \leqslant \eta, |u_2| \leqslant \eta, \max(u,v) \geqslant L$, 则得

$$\begin{aligned}&\frac{\partial^2}{\partial u^2}\sqrt{\{(u+u_1)^2 + (v+v_1)^2\}} \\ =& \frac{(v+v_1)^2}{\{(u+u_1)^2 + (v+v_1)^2\}^{\frac{3}{2}}} \\ =& \frac{v^2}{(u^2+v^2)^{\frac{3}{2}}}\left(1 + \frac{2v_1}{v} + \frac{v_1^2}{v^2}\right)\left(1 + 2\frac{uu_1 + vv_1}{u^2+v^2} + \frac{u_1^2+v_1^2}{u^2+v^2}\right)^{-\frac{3}{2}}\end{aligned}$$

$$= \frac{v^2}{(u^2+v^2)^{\frac{3}{2}}}\left(1+\frac{2v_1}{v}+\frac{v_1^2}{v^2}\right)\left\{1-3\frac{uu_1+vv_1}{u^2+v^2}-\frac{3}{2}\frac{u_1^2+v_1^2}{u^2+v^2}\right.$$

$$\cdot\frac{15}{2}\left(\frac{uu_1+vv_1}{u^2+v^2}\right)^2+\frac{15}{2}\frac{(uu_1+vv_1)(u_1^2+v_1^2)}{(u^2+v^2)^2}-\frac{35}{2}\left(\frac{uu_1+vv_1}{u^2+v^2}\right)^3+\frac{15}{8}\left(\frac{u_1^2+v_1^2}{u^2+v^2}\right)$$

$$\left.-\frac{105}{4}\frac{(uu_1+vv_1)^2(u_1^2+v_1^2)}{(u^2+v^2)^3}+\frac{315}{8}\left(\frac{uu_1+vv_1}{u^2+v^2}\right)^4+\cdots\right\}. \tag{7}$$

命 $G(u,v)=\Delta\{\sqrt{(u^2+v^2)}\}$, 则由 (7) 可知

$$\begin{aligned}G_{uu} = \frac{v^2}{(u^2+v^2)^{\frac{5}{2}}}&\left\{\frac{15}{2}\frac{(X+Z)u+(Y+W)v}{u^2+v^2}\right.\\ &-\frac{35}{2}\frac{Xu^3+3Yu^2v+3Zuv^2+Wv^3}{(u^2+v^2)^2}-3\frac{Y+W}{v}\\ &\left.+15\frac{Yu^2+2Zuv+Wv^2}{v(u^2+v^2)}-3\frac{Zu+Wv}{v^2}\right\}\\ &+O\left(\frac{(|X|+|Y|+|Z|+|W|)\eta}{L^5}\right).\end{aligned}$$

类似地, 我们有

$$\begin{aligned}G_{rr} = \frac{u^2}{(u^2+v^2)^{\frac{5}{2}}}&\left\{\frac{15}{2}\frac{(X+Z)u+(Y+W)v}{u^2+v^2}\right.\\ &-\frac{35}{2}\frac{Xu^3+3Yu^2v+3Zuv^2+Wv^3}{(u^2+v^2)^2}-3\frac{X+Z}{u}\\ &\left.+15\frac{Xu^2+2Yuv+Zv^2}{u(u^2+v^2)}-3\frac{Xu+Yv}{u^2}\right\}\\ &+O\left(\frac{(|X|+|Y|+|Z|+|W|)\eta}{L^5}\right).\end{aligned}$$

及

$$\begin{aligned}G_{ur} = -\frac{uv}{(u^2+v^2)^{\frac{5}{2}}}&\left\{\frac{15}{2}\frac{(X+Z)u+(Y+W)v}{u^2+v^2}\right.\\ &-\frac{35}{2}\frac{Xu^3+3Yu^2v+3Zuv^2+Wv^3}{(u^2+v^2)^2}-\frac{3}{2}\left(\frac{X+Z}{u}+\frac{Y+W}{v}\right)\\ &+\frac{15}{2}\left(\frac{Xu^2+2Yuv+Zv^2}{u(u^2+v^2)}+\frac{Yu^2+2Zuv+Wv^2}{v(u^2+v^2)}\right)\\ &\left.-3\frac{Yu+Zv}{uv}\right\}+O\left(\frac{(|X|+|Y|+|Z|+|W|)\eta}{L^5}\right).\end{aligned}$$

所以

$$G_{uu}G_{vv}-G_{uv}^2$$

$$
\begin{aligned}
&= \frac{u^2v^2}{(u^2+v^2)^5}\Big[\Big\{\frac{15}{2}\frac{(X+Z)u+(Y+W)v}{u^2+v^2} \\
&\quad - \frac{35}{2}\frac{Xu^3+3Yu^2v+3Zuv^2+Wv^3}{(u^2+v^2)^2} - 3\frac{Y+W}{v} \\
&\quad + 15\frac{Yu^2+2Zuv+Wv^2}{v(u^2+v^2)^2} - 3\frac{Zu+Wv}{v^2}\Big\} \\
&\quad \cdot \Big\{\frac{15}{2}\frac{(X+Z)u+(Y+W)v}{u^2+v^2} - \frac{35}{2}\frac{Xu^3+3Yu^2v+3Zuv^2+Wv^3}{(u^2+v^2)^2} \\
&\quad - 3\frac{X+Z}{u} + 15\frac{Xu^2+2Yuv+Zv^2}{u(u^2+v^2)} - 3\frac{Xu+Yv}{u^2}\Big\} \\
&\quad - \Big\{\frac{15}{2}\frac{(X+Z)u+(Y+W)v}{u^2+v^2} \\
&\quad - \frac{35}{2}\frac{Xu^3+3Yu^2v+3Zuv^2+Wv^3}{(u^2+v^2)^2} - \frac{3}{2}\left(\frac{X+Z}{u}+\frac{Y+W}{v}\right) \\
&\quad + \frac{15}{2}\left(\frac{Xu^2+2Yuv+Zv^2}{u(u^2+v^2)} + \frac{Yu^2+2Zuv+Wv^2}{v(u^2+v^2)}\right) \\
&\quad - 3\frac{Yu+Zv}{uv}\Big\}^2\Big] + O\left(\frac{(X^2+Y^2+Z^2+W^2)\eta}{L^9}\right) \\
&= \frac{u^2v^2}{(u^2+v^2)^5}\Big[\Big(\frac{15}{2}\frac{(X+Z)u+(Y+W)v}{u^2+v^2} - \frac{35}{2}\frac{Xu^3+3Yu^2v+3Zuv^2+Wv^3}{(u^2+v^2)^2}\Big) \\
&\quad \times \left(-3\frac{Xu+Yv}{u^2} - 3\frac{Zu+Wv}{v^2} + 6\frac{Yu+Zv}{uv}\right) \\
&\quad + 9\left(\frac{X+Z}{u} - 5\frac{Xu^2+2Yuv+Zv^2}{u(u^2+v^2)} + \frac{Xu+Yv}{u^2}\right) \\
&\quad \times \left(\frac{Y+W}{v} - 5\frac{Yu^2+2Zuv+Wv^2}{v(u^2+v^2)} + \frac{Zu+Wv}{v^2}\right) \\
&\quad - \frac{9}{4}\Big\{\frac{X+Z}{u} + \frac{Y+W}{v} - 5\left(\frac{Xu^2+2Yuv+Zv^2}{u(u^2+v^2)} + \frac{Yu^2+2Zuv+Wv^2}{v(u^2+v^2)}\right) \\
&\quad + 2\frac{Yu+Zv}{uv}\Big\}^2\Big] + O\left(\frac{(X^2+Y^2+Z^2+W^2)\eta}{L^9}\right) \\
&= -\frac{3}{4(u^2+v^2)^7}Q(X,Y,Z,W) + O\left(\frac{(X^2+Y^2+Z^2+W^2)\eta}{L^9}\right)\ (\text{定义}).
\end{aligned}
$$

从而

$$
\begin{aligned}
&-\frac{3}{4}Q(X,Y,Z,W) \\
&= -3\Big[\frac{15}{2}(u^2+v^2)\{(X+Z)u+(Y+W)v\} \\
&\quad - \frac{35}{2}(Xu^3+3Yu^2v+3Zuv^2+Wv^3)\Big]
\end{aligned}
$$

$$
\begin{aligned}
&\times\{v^2(Xu+Yv)+u^2(Zu+Wv)-2uv(Yu+Zv)\}\\
&+9\{u(u^2+v^2)(X+Z)-5u(Xu^2+2Yuv+Zv^2)+(u^2+v^2)(Xu+Yv)\}\\
&\times\{v(u^2+v^2)(Y+W)-5v(Yu^2+2Zuv+Wv^2)+(u^2+v^2)(Zu+Wv)\}\\
&-\frac{9}{4}\{v(u^2+v^2)(X+Z)+u(u^2+v^2)(Y+W)\\
&-5v(Xu^2+2Yuv+Zv^2)-5u(Yu^2+2Zuv+Wv^2)+2(u^2+v^2)(Yu+Zv)\}^2\\
=&-3\left\{\left(-10u^3+\frac{15}{2}uv^2\right)X+\left(-45u^2v+\frac{15}{2}v^3\right)Y\right.\\
&\left.+\left(\frac{15}{2}u^3-45uv^2\right)Z+\left(\frac{15}{2}u^2v-10v^3\right)W\right\}\\
&\times\{uv^2X-(2u^2v-v^3)Y-(-u^3+2uv^2)Z+u^2vW\}\\
&+9\{(-3u^3+2uv^2)X+(-9u^2v+v^3)Y+(u^3-4uv^2)Z\}\\
&\times\{(-4u^2v+v^3)Y+(u^3-9uv^2)Z+(2u^2v-3v^3)W\}\\
&-\frac{9}{4}\{(-4u^2v+v^3)X+(-2u^3-7uv^2)Y+(-7u^2v-2v^3)Z+(u^3-4uv^2)W\}^2\\
=&-\frac{3}{4}(8u^4+6u^2v^2+3v^4)v^2X^2-\frac{9}{4}(4u^6+4u^4v^2+21u^2v^4+6v^6)Y^2\\
&-\frac{9}{4}(6u^6+21u^4v^2+4u^2v^4+4v^6)Z^2-\frac{3}{4}(3u^4+6u^2v^2+8v^4)u^2W^2\\
&-\frac{3}{2}uv(-8u^4+4u^2v^2-3v^4)XY\\
&-\frac{3}{2}uv(-3u^4+4u^2v^2-8v^4)ZW\\
&+\frac{3}{2}(2u^6+20u^4v^2+9u^2v^4+6v^6)XZ\\
&+\frac{3}{2}(6u^6+9u^4v^2+20u^2v^4+2v^6)YW\\
&-\frac{3}{2}(4u^4+3u^2v^2+4v^4)uvXW+\frac{135}{2}u^3v^3YZ.
\end{aligned}
$$

因此

$$
\begin{aligned}
Q(X,Y,Z,W)=&(8u^4+6u^2v^2+3v^4)v^2X^2+3(4u^6+4u^4v^2+21u^2v^4+6v^6)Y^2\\
&+3(6u^6+21u^4v^2+4u^2v^4+4v^6)Z^2\\
&+(3u^4+6u^2v^2+8v^4)u^2W^2-2uv(8u^4-4u^2v^2+3v^4)XY\\
&-2uv(3u^4-4u^2v^2+8v^4)ZW-2(2u^6+20u^4v^2+9u^2v^4+6v^6)XZ\\
&-2(6u^6+9u^4v^2+20u^2v^4+2v^6)YW\\
&+2(4u^4+3u^2v^2+4v^4)uvXW-90u^3v^3YZ. \qquad (8)
\end{aligned}
$$

3. 我们置 $n_1=0$, 则 $W=0$, 所以

$$\begin{aligned}Q(X,Y,Z,0)=&(8u^4+6u^2v^2+3v^4)v^2X^2+3(4u^6+4u^4v^2+21u^2v^4+6v^6)Y^2\\&+3(6u^6+21u^4v^2+4u^2v^4+4v^6)Z^2\\&-2uv(8u^4-4u^2v^2+3v^4)XY\\&-2(2u^6+20u^4v^2+9u^2v^4+6v^6)XZ-90u^3v^3YZ.\end{aligned}$$

本节的目的为证明

$$Q(X,Y,Z,0)\geqslant\frac{1}{10}\{(u^2+v^2)^2v^2X^2+(u^2+v^2)^3(Y^2+Z^2)\}.$$

当 $v\geqslant u$ 时, 有

$$Q(X,Y,Z,0)\geqslant\frac{1}{20}(u^2+v^2)^3(X^2+Y^2+Z^2).$$

我们显然有

$$Y^2=4m_1^2(m_2n_3+m_3n_2)^2\geqslant 16m_1^2m_2m_3n_2n_3=\frac{4}{3}XZ. \tag{9}$$

由于

$$\begin{aligned}&(79u^4+58u^2v^2+29v^4)(89u^4-183u^2v^2+312v^4)\\&-10^2(8u^4-4u^2v^2+3v^4)^2\\\geqslant&600u^8-3000u^6v^2+10000u^4v^4\geqslant 0\end{aligned}$$

与

$$\begin{aligned}&(180u^2+89v^2)(179u^2+627v^2)-450^2u^2r^2\\\geqslant&\{2\sqrt{180\cdot179\cdot89\cdot627)}+179.89+180.627-450^2)u^2v^2\geqslant 0.\end{aligned}$$

所以

$$\begin{aligned}Q(X,Y,Z,0)\geqslant&(8u^4+6u^2v^2+3v^4)v^2X^2\\&+9\left(u^6-2u^4v^2+\frac{11}{2}u^2v^4+v^6\right)Y^2\\&+3(6u^6+21u^4v^2+4u^2v^4+4v^6)Z^2\\&-2uv(8u^4-4u^2v^2+3v^4)XY-90u^3v^3YZ\\\geqslant&\frac{1}{10}\{(u^2+v^2)^2v^2X^2+(u^2+v^2)^3(Y^2+Z^2)\}\end{aligned}$$

$$
\begin{aligned}
&+\left(\frac{79}{10}u^4+\frac{58}{10}u^2v^2+\frac{29}{10}v^4\right)v^2X^2\\
&-2uv\left(8u^4-4u^2v^2+3v^3\right)XY\\
&+\left(\frac{89}{10}u^4-\frac{183}{10}u^2v^2+\frac{312}{10}v^4\right)u^2Y^2\\
&+\left(18u^2+\frac{89}{10}v^2\right)v^4Y^2+\left(\frac{179}{10}u^2+\frac{627}{10}v^2\right)u^4Z^2\\
&-90u^3v^3YZ\\
\geqslant&\ \frac{1}{10}\{(u^2+v^2)^2v^2X^2+(u^2+v^2)^3(Y^2+Z^2)\},
\end{aligned}
$$

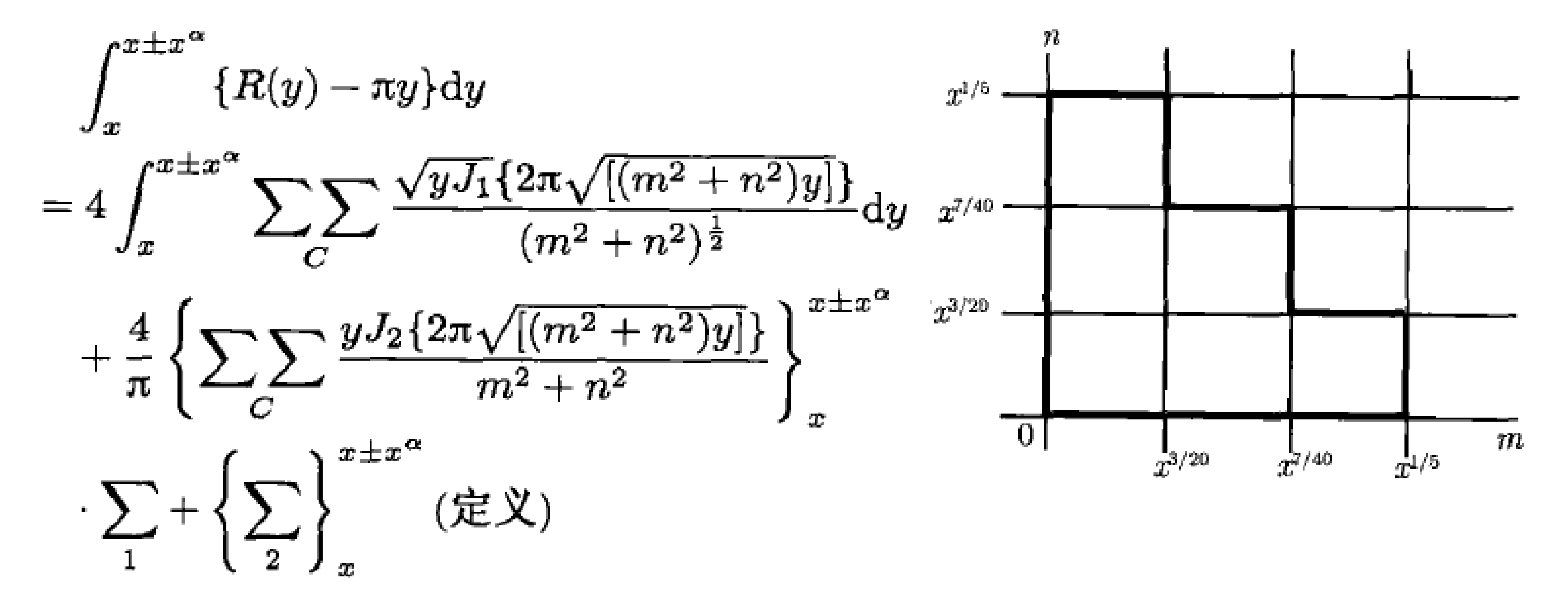
4. 熟知

$$
\int_0^x\{R(y)-\pi y\}\mathrm{d}y=\frac{x}{\pi}\sum_{v=1}^{\infty}\frac{r(v)}{v}J_2\{2\pi\sqrt{(vx)}\},
$$

此处 $r(v)$ 表示丢番图方程 $x^2+y^2=v$ 的解数, 显然有

$$
\int_0^x\{R(y)-\pi y\}\mathrm{d}y=\frac{4x}{\pi}\sum_{m=1}^{\infty}\sum_{n=0}^{\infty}\frac{J_2\{2\pi\sqrt{[(m^2+n^2)x]}\}}{m^2+n^2}.
$$

命 $C$ 表示图中重黑线所包围的区域及 $C'$ 表示在第一象限中其余的部分, 则易于推出: 若 $0<\alpha<1$(以后我们将置 $\alpha=13/40$), 则




$$
\begin{aligned}
&\int_x^{x\pm x^\alpha}\{R(y)-\pi y\}\mathrm{d}y\\
=&\ 4\int_x^{x\pm x^\alpha}\sum_C\sum\frac{\sqrt{y}J_1\{2\pi\sqrt{[(m^2+n^2)y]}\}}{(m^2+n^2)^{\frac12}}\mathrm{d}y\\
&+\frac{4}{\pi}\left\{\sum_C\sum\frac{yJ_2\{2\pi\sqrt{[(m^2+n^2)y]}\}}{m^2+n^2}\right\}_x^{x\pm x^\alpha}\\
&\cdot\sum_1+\left\{\sum_2\right\}_x^{x\pm x^\alpha}\quad(\text{定义})
\end{aligned}
$$

现在

$$
J_1\{2\pi\sqrt{(vy)}\}=\frac{\sin\left\{2\pi\sqrt{(vy)}-\frac14\pi\right\}}{\pi(vy)^{\frac14}}+O\left(\frac{1}{(vy)^{\frac34}}\right).
$$

所以

$$
\sum_1=O\left(\int_x^{x\pm x^\alpha}|\phi(y)|y^{\frac14}\mathrm{d}y\right)+O(x^{\alpha-\frac14}),
$$

此处

$$\phi(y)=\sum_C\sum\frac{e^{2\pi i\sqrt{\{(m^2+n^2))y\}}}}{(m^2+n^2)^{\frac34}}\quad(x-x^\alpha\leqslant y\leqslant x+x^\alpha).\tag{10}$$

类似地, 我们有

$$\sum_2=O\{y^{\frac34}|\psi(y)|\}+O(x^{\frac14}),$$

此处

$$\psi(y)=\sum_{C'}\sum\frac{e^{2\pi i\sqrt{\{(m^2+n^2))y\}}}}{(m^2+n^2)^{\frac54}}\quad(x-x^\alpha\leqslant y\leqslant x+x^\alpha).\tag{11}$$

若 $m\leqslant x^{\frac{3}{20}}$, 则

$$\begin{aligned}y^{\frac14}\left|\sum_{\substack{C\\ m\leqslant x^{\frac13}}}\sum\frac{e^{2\pi i\sqrt{\{(m^2+n^2)v\}}}}{(m^2+n^2)^{\frac34}}\right|&\leqslant y^{\frac14}\sum_{m\leqslant x^{\frac{3}{20}}}\sum_{n=1}^{\infty}\frac{1}{(m^2+n^2)^{\frac34}}\\&\leqslant y^{\frac14}\sum_{m\leqslant x^{\frac{3}{20}}}\left(\sum_{n=1}^{m}\frac{1}{n^{\frac32}}+\sum_{n=m+1}^{\infty}\frac{1}{n^{\frac32}}\right)\\&=O\left(y^{\frac14}\sum_{m\leqslant x^{\frac{3}{20}}}m^{-\frac12}\right)=O(x^{\frac14+\frac{3}{40}})=O(x^\alpha).\end{aligned}$$

同样的结果对于 $n\leqslant x^{\frac{3}{20}}$ 成立.

若 $m\geqslant x^{\frac15}$, 则

$$y^{\frac34}\left|\sum_{\substack{C'\\ m\geqslant x^{\frac13}}}\sum\frac{e^{2\pi i\sqrt{\{(m^2+n^2)y\}}}}{(m^2+n^2)^{\frac54}}\right|\leqslant y^{\frac34}\sum_{m\geqslant x^{\frac13}}\left(\frac{1}{m^{\frac32}}\right)=O(x^{\frac34-\frac{1}{10}})=O(x^{2\alpha}).$$

同样的结果对于 $n\geqslant x^{\frac15}$ 成立.

命 $D$ 表示 $C$ 与方形

$$x^{\frac{3}{20}}\leqslant m,\quad n\leqslant x^{\frac15}$$

的公共部分, 及 $D'$ 表示方形中的余下部分, 则

$$y^{\frac14}|\phi(y)|=y^{\frac14}|\sum_D\sum\frac{e^{2\pi i\sqrt{\{(m^2+n^2)y\}}}}{(m^2+n^2)^{\frac34}}|+O(x^\alpha)\tag{12}$$

与

$$y^{\frac34}|\psi(y)|=y^{\frac34}\left|\sum_{D'}\sum\frac{e^{2\pi i\sqrt{\{(m^2+n^2)y\}}}}{(m^2+n^2)^{\frac54}}\right|+O(x^{2\alpha}).\tag{13}$$

5. 现在考虑形如

$$S=\sum_{m=M}^{M'}\sum_{n=N}^{N'}\mathrm{e}^{2\pi\mathrm{i}f(m,n)},\quad M\leqslant M'\leqslant 2M;\quad N\leqslant N'\leqslant 2N$$

的和, 此处 $f(m,n)=\sqrt{\{(m^2+n^2)y\}}$. 命 $R$ 表示求和区域及 $L=\max(m,n)$. 我们考虑的项满足

$$x^{\frac{3}{20}}<L<x^{\frac{1}{5}}. \tag{14}$$

若 $M'-M<x^{\frac{1}{8}}$, 则 $S=O(Lx^{\frac{1}{8}})$, 所以由引理 1 得

$$x^{\frac{1}{4}}\sum_R\sum\frac{\mathrm{e}^{2\pi\mathrm{i}f(m,n)}}{(m^2+n^2)^{\frac{3}{4}}}=O(x^{\frac{1}{4}+\frac{1}{8}}L^{-\frac{1}{2}})=O(x^{\frac{1}{4}+\frac{1}{8}-\frac{3}{40}})=O(x^{\alpha}) \tag{15}$$

及

$$x^{\frac{3}{4}}\sum_R\sum\frac{\mathrm{e}^{2\pi\mathrm{i}f(m,n)}}{(m^2+n^2)^{\frac{5}{4}}}=O(x^{\frac{3}{4}+\frac{1}{8}}L^{-\frac{3}{2}})=O(x^{\frac{3}{4}+\frac{1}{8}-\frac{9}{40}})=O(x^{2\alpha}). \tag{16}$$

若 $N'-N<x^{\frac{1}{8}}$, 则得一个类似的结果, 所以我们可以假定

$$M'-M>x^{\frac{1}{8}},\quad N'-N>x^{\frac{1}{8}}.$$

应用引理 2′ 一次及引理 2 二次得

$$\begin{aligned}S&=O(L^2\rho^{-\frac{1}{2}})+O\left[L\rho^{-\frac{1}{2}}\left(\sum_{m_1=1}^{\rho-1}|S_1|^{\frac{1}{2}}\right)\right]\\&=O(L^2\rho^{-\frac{1}{2}})+O\left[L^{\frac{3}{2}}\rho^{-1}\sum_{i=1}^{2}\left\{\sum_{m_1=1}^{\rho-1}\left(\sum_{m_2=1}^{\rho-1}\sum_{n_2=0}^{\rho-1}|S_2^{(i)}|\right)^{\frac{1}{2}}\right\}^{\frac{1}{2}}\right]\\&=O(L^2\rho^{-\frac{1}{2}})+O\left[L^{\frac{7}{4}}\rho^{-\frac{3}{2}}\sum_{i=1}^{4}\left\{\sum_{m_1=1}^{\rho-1}\left[\sum_{m_2=1}^{\rho-1}\sum_{n_2=0}^{\rho-1}\left(\sum_{m_2=1}^{\rho^2-1}\sum_{n_2=0}^{\rho^2-1}|S_3^{(i)}|\right)^{\frac{1}{2}}\right]^{\frac{1}{2}}\right\}^{\frac{1}{2}}\right],\end{aligned} \tag{17}$$

在此需假定

$$1\leqslant\rho^2\leqslant\frac{1}{2}x^{\frac{1}{8}},$$

$$S_3^{(1)}=S_3=\sum\sum\mathrm{e}^{2\pi\mathrm{i}g(m,n)},\quad g(m,n)=\sqrt{x}G(m,n), \tag{18}$$

$W=0$, 及 $S_3^{(2)}, S_3^{(3)}, S_3^{(4)}$ 分别对应于和, 以 $(-m_3, n_3), (m_3, -n_3)(-m_3, -n_3)$ 代替 $(m_3, n_3)$. 我们可以假定 $v>u$(由对称性). 由 §3 可知

$$g_{uu}g_{vv}-g_{uv}^2 \geqslant \frac{x}{L^8}(X^2+Y^2+Z^2)+O\left(\frac{(X^2+Y^2+Z^2)x\eta}{L^9}\right)$$
$$\geqslant A\frac{x}{L^8}(X^2+Y^2+Z^2),$$

此处 $A$ 为某常数, 在此需假定

$$\rho=O(L^{\frac{1}{2}}). \tag{19}$$

事实上, 由于 $\eta=O(\rho^2)$, 所以

$$\frac{(X^2+Y^2+Z^2)x\eta}{L^9}=O\left(\frac{x(X^2+Y^2+Z^2)\rho^2}{L^9}\right)=O\left(\frac{x(X^2+Y^2+Z^2)}{L^8}\right).$$

6. 由于 $X=O(\rho^4), Y=O(\rho^4), Z=O(\rho^4)$, 所以

$$g_{uu}=O\left(\frac{x^{\frac{1}{2}}\rho^4}{L^4}\right)+O\left(\frac{x^{\frac{1}{2}}\rho^4\eta}{L^5}\right)=O\left(\frac{x^{\frac{1}{2}}\rho^4}{L^4}\right),$$

其中 $\eta=O(\rho^2)=O(L)$. 对于 $g_{vv}$ 与 $g_{uv}$, 类似的结果成立. 因此, 若

$$l=aL^4x^{-\frac{1}{2}}\rho^{-4},$$

其中 $a$ 充分小, $a$ 为 $g_u$ 与 $g_v$ 在一个边长 $l$ 小于 $\frac{1}{2}$ 的方形中的变差, 假定将 $S_3$ 的求和区域分割成这种方形及这种方形的一部分, 则对于整数 $\mu, \nu$ 的每一个方形满足: 若

$$h(u,v)=g(u,v)-\mu u-\upsilon v,$$

则 $|h_u|\leqslant\frac{3}{4}, |h_v|\leqslant\frac{3}{4}$, 所以由引理 3 可知对于每一个方形

$$\sum\sum e^{2\pi i g(m,n)}=\iint e^{2\pi i h(u,v)}\mathrm{d}u\mathrm{d}v+O(l).$$

由 §5, 我们可以在引理 4 中取

$$r^2=A\frac{x}{L^8}(X^2+Y^2+Z^2).$$

同样

$$r_1=O(1), r_3=O(x^{\frac{1}{2}}\rho^4L^{-5}),$$

所以若

$$L^3\rho^4<K_1Ax^{\frac{1}{2}}(X^2+Y^2+Z^2). \tag{20}$$

则引理 4 中的条件 (5) 满足.

引理 4 亦要求 $lr_3 < K_2r$, 即

$$L^6 < K_2(X^2+Y^2+Z^2)x. \tag{21}$$

由于 $X^2+Y^2+Z^2=O(\rho^8)$, 所以若 (20) 满足, 则 (21) 满足, 因此若 (20) 成立, 并假定 $L=O(x^4)$, 则由引理 4 得

$$\int\int \mathrm{e}^{2\pi \mathrm{i}h(u,v)}\mathrm{d}u\mathrm{d}v = O\left(\frac{L^2\log x}{x^{\frac{1}{2}}(X^2+Y^2+Z^2)^{\frac{1}{2}}}\right),$$

假定 $l\leqslant L$, 则这种项数为 $O(L^2/l^2)$, 所以在限制 (20) 之下有

$$\begin{aligned} S_3 &= O\left(\frac{L^6\log x}{l^2x^{\frac{1}{2}}(X^2+Y^2+Z^2)^{\frac{1}{2}}}\right)+O\left(\frac{L^2}{l}\right) \\ &= O\left(\frac{x^{\frac{1}{2}}\rho^8\log x}{L^2(X^2+Y^2+Z^2)^{\frac{1}{2}}}\right)=O\left(\frac{x^{\frac{1}{2}}\rho^8\log x}{L^2m_1m_2m_3}\right), \end{aligned} \tag{22}$$

这一结果对于 $S_3^{(i)}(i=2,3,4)$ 当然亦成立.

7. 假定 (20) 成立, 则将 (22) 代入 (17) 可知当 $v\geqslant u$ 时

$$\begin{aligned} &O\left(\frac{L^{\frac{7}{4}}}{\rho^{\frac{3}{2}}}\left\{\sum_{m_1=1}^{\rho-1}\left[\sum_{m_2=1}^{\rho-1}\sum_{n_2=0}^{\rho-1}\left(\sum_{m_2=1}^{\rho^2-1}\sum_{n_2=0}^{\rho^2-1}|S_3|\right)^{\frac{1}{2}}\right]^{\frac{1}{2}}\right\}^{\frac{1}{2}}\right) \\ &= O\left(\frac{L^{\frac{7}{4}}}{\rho^{\frac{3}{2}}}\left(\frac{x^{\frac{1}{2}}\rho^8\log x}{L^2}\right)^{\frac{1}{8}}\left\{\sum_{m_1=1}^{\rho-1}\left[\sum_{m_2=1}^{\rho-1}\sum_{n_2=0}^{\rho-1}\left(\sum_{m_3=1}^{\rho^2-1}\sum_{n_3=0}^{\rho^2-1}\frac{1}{m_1m_2m_3}\right)^{\frac{1}{2}}\right]^{\frac{1}{2}}\right\}^{\frac{1}{2}}\right) \\ &= O\{L^{\frac{3}{2}}\rho^{-\frac{1}{2}}x^{\frac{1}{16}}(\log x)^{\frac{1}{8}}\cdot\rho(\log\rho)^{\frac{1}{8}}\} \\ &= O\{L^{\frac{3}{2}}\rho^{\frac{1}{2}}x^{\frac{1}{16}}(\log x)^{\frac{1}{4}}\}, \end{aligned}$$

其次, 我们考虑不适合 (20) 之诸项之和, 我们得不等式

$$X^2+Y^2+Z^2=O(L^3\rho^4x^{-\frac{1}{2}}).$$

从而 $m_1m_2m_2=O(L^3\rho^4x^{-\frac{1}{2}}), m_1n_2n_3=O(L^3\rho^4x^{-\frac{1}{2}})$. 由于 $S_3=O(L^2)$, 所以不满足 (20) 之诸项之和等于

$$O\left(L^{\frac{7}{4}}\rho^{-\frac{3}{2}}\left\{\sum_{m_1=1}^{\rho-1}\left[\sum_{m_2=1}^{\rho-1}\sum_{n_2=1}^{\rho-1}\left(\sum_{m_3=O(L^{\frac{3}{2}}\rho^2x^{-\frac{1}{4}}m_1^{-1}m_2^{-1})}\right.\right.\right.\right.$$

$$\left.\left.\left.\left.\times \sum_{n_3=O(L^{\frac{3}{2}}\rho^2x^{-\frac{1}{4}}m_1^{-1})n_2^{-1}} 1\right)^{\frac{1}{2}}\right]^{\frac{1}{2}}\right\}^{\frac{1}{2}}\right)$$

$$= O\left(L^{\frac{7}{4}}\rho^{-\frac{3}{2}}\left\{\sum_{m_1=1}^{\rho-1}\left[\sum_{m_2=1}^{\rho-1}\sum_{n_2=1}^{\rho-1} L^{\frac{3}{2}}\rho^2x^{-\frac{1}{4}}m_1^{-1}m_2^{-\frac{1}{2}}n_2^{-\frac{1}{2}}\right]^{\frac{1}{2}}\right\}^{\frac{1}{2}}\right)$$

$$= O\left(L^{\frac{17}{8}}\rho^{-1}x^{-\frac{1}{16}}\left[\sum_{m_1=1}^{\rho-1}\left(\sum_{m_2=1}^{\rho-1}\sum_{n_2=1}^{\rho-1}\frac{1}{(m_2n_2)^{\frac{1}{2}}}\right)^{\frac{1}{2}}\frac{1}{m_1^{\frac{1}{2}}}\right]^{\frac{1}{2}}\right)$$

$$= O(L^{\frac{17}{8}}\rho^{-1}x^{-\frac{1}{16}}\rho^{\frac{1}{2}}) = O(L^{\frac{17}{8}}\rho^{-\frac{1}{2}}x^{-\frac{1}{16}}).$$

(满足 $n_2 = 0$ 之诸项之和为一个低阶) 当 $v < u$ 时, 类似的结果成立, 所以

$$S = O(L^2\rho^{-\frac{1}{2}}) + O\{L^{\frac{3}{2}}\rho^{\frac{1}{2}}x^{\frac{1}{16}}(\log x)^{\frac{1}{4}}\} + O(L^{\frac{17}{8}}\rho^{-\frac{1}{2}}x^{-\frac{1}{16}}).$$

若

$$\rho = [L^{\frac{1}{2}}x^{-\frac{1}{16}}(\log x)^{-\frac{1}{4}}],$$

则前两项具有同样的形式. 若这是 $\rho$ 可以允许的数值, 则得

$$\begin{aligned} S &= O\{L^{\frac{7}{4}}x^{\frac{1}{32}}(\log x)^{\frac{1}{8}}\} + O\{L^{\frac{15}{8}}x^{-\frac{1}{32}}(\log x)^{\frac{1}{8}}\} \\ &= O\{L^{\frac{7}{4}}x^{\frac{1}{32}}(\log x)\}^{\frac{1}{8}}. \end{aligned} \tag{23}$$

现在, 我们来验证所有的条件, 条件 (18)

$$1 \leqslant \rho^2 = Lx^{-\frac{1}{8}}(\log x)^{-\frac{1}{2}} \leqslant \frac{1}{2}x^{\frac{1}{8}}$$

可以写成

$$x^{\frac{1}{8}}(\log x)^{\frac{1}{2}} \leqslant L \leqslant x^{\frac{1}{4}}(\log x)^{\frac{1}{2}}.$$

由于 $\frac{1}{8} < \frac{3}{20} < \frac{1}{5} < \frac{1}{4}$, 所以这总能成立. 条件 (19) 为

$$L^{\frac{1}{2}}x^{-\frac{1}{16}}(\log x)^{-\frac{1}{4}} - 1 \leqslant \rho = O(L^{\frac{1}{2}}).$$

这总是能满足的.

8. 由引理 1 及 (23) 可知

$$\sum_R\sum \frac{e^{2\pi i\sqrt{\{(m^2+n^2)y\}}}}{(m^2+n^2)^{\frac{3}{4}}} = O\{L^{\frac{7}{4}-\frac{3}{2}}x^{\frac{1}{32}}(\log x)^{\frac{1}{8}}\} \tag{24}$$

与

$$\sum_R\sum \frac{e^{2\pi i\sqrt{\{(m^2+n^2)y\}}}}{(m^2+n^2)^{\frac{5}{4}}} = O\{L^{\frac{7}{4}-\frac{5}{2}}x^{\frac{1}{32}}(\log x)^{\frac{1}{8}}\}. \tag{25}$$

现在我们将和分拆成

$$\sum_D\sum \frac{e^{2\pi i\sqrt{\{(m^2+n^2)y\}}}}{(m^2+n^2)^{\frac{3}{4}}} = \sum_{p=1}^{P}\sum_{q=1}^{Q}\left\{\sum_{2^{p-1}}^{2^p}\sum_{2^{q-1}}^{2^q}\frac{e^{2\pi i\sqrt{\{(m^2+n^2)y\}}}}{(m^2+n^2)^{\frac{3}{4}}}\right\}.$$

取 $L_0 = x^{\frac{7}{40}}$, 则由 (12) 与 (24) 得

$$\begin{aligned} y^{\frac{1}{4}}|\phi(y)| &= O\left(x^{\frac{1}{4}}\sum_{p=1}^{P}\sum_{q=1}^{Q}\{\max(2^p,2^q)\}^{\frac{1}{4}}x^{\frac{1}{32}}(\log x)^{\frac{1}{8}}\right) + O(x^{\alpha}) \\ &= O\{x^{\frac{9}{32}}L_0^{\frac{1}{4}}(\log x)^{\frac{9}{8}}\} + O(x^{\alpha}) \\ &= O\{x^{\alpha}(\log x)^{\frac{9}{8}}\}. \end{aligned}$$

类似地, 由 (13) 与 (25) 得

$$\begin{aligned} y^{\frac{3}{4}}|\psi(y)| &= O\left(x^{\frac{3}{4}}\sum_{p=1}^{P}\sum_{q=1}^{Q}\{\max(2^p,2^q)\}^{-\frac{3}{4}}x^{\frac{1}{32}}(\log x)^{\frac{1}{8}}\right) + O(x^{\frac{1}{4}+\alpha}) \\ &= O\{x^{\frac{26}{40}}(\log x)^{\frac{9}{8}}\} + O(x^{\frac{1}{4}+\alpha}) \\ &= O\{x^{2\alpha}(\log x)^{\frac{9}{8}}\}. \end{aligned}$$

所以得

$$\int_x^{x\pm x^{\alpha}}\{R(y)-\pi y\}\mathrm{d}y = O\{x^{2\alpha}(\log x)^{\frac{9}{8}}\}.$$

因此用通常的方法即易于得到

$$R(x) = \pi x + O\{x^{\frac{13}{40}}(\log x)^{\frac{9}{8}}\}.$$

(王元 译)

# 关于二次非剩余的分布及实二次域中的欧几里得算法（Ⅰ）①

华罗庚（昆明国立清华大学）

## 1. 导　言

本文的目的之一为建立一个 mod $p$ 的最小二次非剩余的确切上界. 这个界是作者能够获得的, 但非最佳者②. 作者得到这一结果是基于以下事实：现在的程序下, 我们可以应用 Rosser③的某些已有结果并足以建立实二次域的 E. A.(欧里几得算法的缩写) 研究的某些典型结果④.

关于 E. A. 研究的结果, 我们证明了以下定理：

**定理**　当 $d > e^{250}$, 在二次域 $R(d^{\frac{1}{2}})$ 中没有 E. A.; 此处 $d$ 为一个平方自由数.

有三条途径可以改进这一结果：(i) 用 Euler 求和公式来改进一个和的估计; (ii) 重新考虑某些特征和的估计, 及 (iii) 用 Riemann-Mangoldt 公式作高阶 "平均" 来平滑关于素数分布的某些结果⑤.

## 2. 征引自 Rosser 文章中的引理

**引理 1**　命

$$\vartheta(x) = \sum_{p \leqslant x} \log p,$$

---

① 1943 年 11 月 29 日收到. 发表于 *Trans. Amer. Math. Soc.*, 1944, 56: 527-546.

② 一个较好的结果已经得到. 例如, 在定理中我们可以有 $d>e^{160}$. 但其证明至少比现在的证明困难十倍.

③ *Amer. J. Math.*, 1941, 63: 211–232.

④ 关于这个问题的历史的详细叙述, 请见 A. Brauer. *Amer. J. Math.*, 1940, 62: 697–713.

⑤ 当附注 (3) 中文章出现后, 只有下面诸情况, E. A. 是否存在尚不得知:

Ⅰ. $d = p$, 此处 $p$ 为形如 $8n + 1$ 的素数, 或 $p = 61$ 及 109.

Ⅱ. $d = p_1p_2 \equiv 1 \pmod{24}$, 此处 $p_1$ 与 $p_2$ 为素数及 $p_1 \equiv p_2 \equiv 3 \pmod 4$. 在这两种情况下皆可知当 $d$ 充分大时, E. A. 不存在, 但同时, Rédei (Über den Euklidischen Algorichmus in reellquadratischen Zahlkörpern. *Mat. Fig. Lapok*, 1940, 47: 78–90) 证明了在情况Ⅱ之下, E. A. 不存在. 作者并不知道 Rédei 的文章; 所以在本文的原稿中, 他考虑了情形Ⅰ与Ⅱ, 但现在情形Ⅱ已无任何兴趣. 在现在条件下, 为了使文章早日面世, 我们未通知作者, 将该文作了一定改动, 即仅有情形Ⅰ. A. Brauer.

此处 $p$ 过所有不超过 $x$ 的素数, 则当 $x\geqslant 1$ 时有

$$\vartheta(x)<(1+0.0376)x,$$

而当 $x\geqslant 51^2$ 时有 $\vartheta(x)>(1-0.0393)x$.

**证明** (1) 由 Rosser 的 (10) 可知, 当 $x\geqslant e^{13.8}$ 时, $\vartheta(x)<(1+0.0376)x$. 至于 $x<e^{13.8}$ 时, 则由 Rosser 的定理 2 得 $\vartheta(x)<x<(1+0.0376)x$.

(2) 由 Rosser 的 (10) 可知当 $x\geqslant e^{13.8}$ 时, $\vartheta(x)>(1-0.0393)x$, 对于 $71^2\leqslant x<e^{13.8}$, 由 Rosser 的定理 7, 得

$$\vartheta(x)>x-2.78x^{\frac{1}{2}}>(1-0.0393)x.$$

当 $51^2\leqslant x<71^2$ 时, 由 Rosser 的定理 5, 得

$$\vartheta(x)>x-2x^{\frac{1}{2}}>(1-0.0393)x.$$

**引理 2** 命

$$\pi(x)=\sum_{p\leqslant x}1,\quad \mathrm{li}x=\lim_{\varepsilon\to 0}\left(\int_0^{1-\varepsilon}+\int_{1+\varepsilon}^{x}\right)\frac{\mathrm{d}y}{\log y}.$$

则当 $x\geqslant 2$ 时, 我们有 $\pi(x)<(1+0.0376)(\mathrm{li}x+1.85)$, 及当 $x\geqslant 51^2$ 时有

$$\pi(x)>(1-0.0393)\mathrm{li}x-1.7.$$

**证明** 我们有恒等式

$$\pi(x)=\frac{\vartheta(x)}{\log x}+\int_2^x\frac{\vartheta(y)\mathrm{d}y}{y\log^2 y}.$$

(1) 由引理 1 并利用 li2=1.04 得

$$\begin{aligned}\pi(x)&<1.0376\left(\frac{x}{\log x}+\int_2^x\frac{\mathrm{d}y}{\log^2 y}\right)\\&=1.0376\left(\int_0^x\frac{\mathrm{d}y}{\log y}+\frac{2}{\log 2}-\int_0^2\frac{\mathrm{d}y}{\log y}\right)\\&<1.0376(\mathrm{li}x+1.85),\end{aligned}$$

(2) 当 $x\geqslant k\geqslant 51^2$ 时, 由恒等式得

$$\begin{aligned}\pi(x)-\pi(K)&=\frac{\vartheta(x)}{\log x}-\frac{\vartheta(K)}{\log K}+\int_K^x\frac{\vartheta(y)\mathrm{d}y}{y(\log y)^2}\\&>\frac{(1-0.0393)x}{\log x}-\frac{\vartheta(K)}{\log K}+(1-0.0393)\int_K^x\frac{\mathrm{d}y}{(\log y)^2}\end{aligned}$$

$$= (1-0.0393)\left(\mathrm{li}x + \frac{K}{\log K} - \mathrm{li}K\right) - \frac{\vartheta(K)}{\log K}.$$

所以

$$\pi(x) > (1-0.0393)(\mathrm{li}x + K/\log K - \mathrm{li}K) \\ - (\vartheta(K)/\log K - \pi(K)).$$

取 $K = 51^2$. 由于

$$\vartheta(K) = 2519.887, \quad \pi(K) = 378, \quad \mathrm{li}(K) = 392.48.$$

故得引理.

**引理 3** 当 $x \geqslant 2$ 时有

$$\vartheta(x)/x \geqslant 0.3465735.$$

**证明** 当 $x \geqslant 16$ 时, 由引理 1 及 Rosser 的定理 6 即得引理. 当 $x \leqslant 16$ 时, 由下面的直接验算即得引理.

$$\vartheta(2)/2 = 0.3465735, \quad \vartheta(3)/3 > \vartheta(4)/4 \geqslant 0.44794,$$

$$\vartheta(5)/5 > \vartheta(6)/6 = 0.56686,$$

$$\vartheta(7)/7 > \vartheta(8)/8 > \vartheta(9)/9 > \vartheta(10)/10 = 0.53471,$$

$$\vartheta(11)/11 > \vartheta(12)/12 = 0.64542,$$

$$\vartheta(13)/13 > \vartheta(14)/14 > \vartheta(15)/15 > \vartheta(16)/16 = 0.64437.$$

## 3. 关于级数的一条引理

**引理 4** 当 $q < A$ 时有

$$\sum_{\nu=1}^{A/q} \mathrm{li}\frac{A}{\nu} \leqslant A \log\frac{\log A}{\log q} + \frac{A}{q}\mathrm{li}q.$$

**证明** 由于 $\mathrm{d}\ \mathrm{li}(A/x)/\mathrm{d}x \leqslant 0$, 所以

$$\sum_{\nu=1}^{A/q} \mathrm{li}\frac{A}{\nu} \leqslant \int_1^{A/q} \mathrm{li}\frac{A}{x}\mathrm{d}x + \mathrm{li}A = \int_1^{A/q}\mathrm{d}x\int_0^{A/x}\frac{\mathrm{d}y}{\log y} + \mathrm{li}A \\ = (A/q)\mathrm{li}q + A\log\log A - A\log\log q.$$

**附记** 引理中的不等式可以由 Euler 求和公式来精密化.

## 4. 关于特征和的引理

**引理 5** 命 $p$ 为一个素数及 $p\equiv 1(\bmod 4)$. 则当 $A<p$ 时, 我们有

$$\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right)\leqslant\frac{1}{2}Ap^{\frac{1}{2}},$$

此处 $\left(\frac{n}{p}\right)$ 表示 Legendre 符号.

**证明** 我们假定 $p<(A+1)^2$. 否则, 我们有

$$\left|\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right)\right|\leqslant\sum_{a=1}^{A}\sum_{n=1}^{a}1=\frac{1}{2}A(A+1)\leqslant\frac{1}{2}Ap^{1/2}.$$

易知

$$\sum_{r=1}^{p}\left(\frac{r}{p}\right)\mathrm{e}^{2\pi\mathrm{i}rn/p}=\left(\frac{n}{p}\right)p^{1/2}.$$

我们有

$$\begin{aligned}p^{\frac{1}{2}}\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right)&=\frac{1}{2}p^{\frac{1}{2}}\sum_{a=0}^{A}\sum_{n=-a}^{a}\left(\frac{n}{p}\right)=\frac{1}{2}\sum_{a=0}^{A}\sum_{n=-a}^{a}\sum_{r=1}^{p}\left(\frac{r}{p}\right)\mathrm{e}^{2\pi\mathrm{i}rn/p}\\&=\frac{1}{2}\sum_{r=1}^{p}\left(\frac{r}{p}\right)\sum_{a=0}^{A}\sum_{n=-a}^{a}\mathrm{e}^{2\pi\mathrm{i}rn/p}\\&=\frac{1}{2}\sum_{r=1}^{p}\left(\frac{r}{p}\right)\frac{\sin^2\pi r(A+1)/p}{\sin^2\pi r/p}.\end{aligned}$$

所以

$$\begin{aligned}p^{\frac{1}{2}}\left|\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right)\right|&\leqslant\frac{1}{2}\sum_{r=1}^{p-1}\frac{\sin^2\pi r(A+1)/p}{\sin^2\pi r/p}\\&=\frac{1}{2}\sum_{r=1}^{p-1}\sum_{a=0}^{A}\sum_{n=-a}^{a}\mathrm{e}^{2\pi\mathrm{i}rn/p}\\&=p(A+1)/2-(A+1)^2/2\leqslant pA/2.\end{aligned}$$

**引理 6** 命 $r_1,r_2,\cdots,r_s$ 为 $s$ 个与 $p$ 不同的素数. 则

$$\left|\sum_{a=1}^{A}\sum_{n=1,(n,r_1,r_2,\cdots,r_s)=1}^{a}\left(\frac{n}{p}\right)\right|\leqslant 2^{s-1}Ap^{\frac{1}{2}}.$$

**证明** 左端的和可以写为

$$\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right)-\sum_{\nu=1}^{s}\sum_{a=1}^{A}\sum_{n=1,r_\nu|n}^{a}\left(\frac{n}{p}\right)$$
$$+\sum_{1\leqslant\nu<\mu\leqslant s}\sum_{a=1}^{A}\sum_{n=1,r_\nu,r_\mu|n}^{a}\left(\frac{n}{p}\right)-\cdots+\cdots.$$

共有 $2^s$ 个和, 每个和具有形式

$$\sum_{a=1}^{A}\sum_{n=1,m|n}^{a}\left(\frac{n}{p}\right).$$

由引理 5 可知

$$\left|\sum_{a=1}^{A}\sum_{n=1,m|n}^{a}\left(\frac{n}{p}\right)\right|=\left|\sum_{a=1}^{A}\sum_{\lambda=1}^{[a/m]}\left(\frac{m\lambda}{p}\right)\right|^{①}$$
$$=\left|\sum_{a=1}^{A}\sum_{\lambda=1}^{[a/m]}\left(\frac{\lambda}{p}\right)\right|\leqslant m\left|\sum_{b=1}^{A/m}\sum_{\lambda=1}^{b}\left(\frac{\lambda}{p}\right)\right|$$
$$\leqslant m\frac{a}{m}p^{1/2}/2=Ap^{1/2}/2.$$

引理证完.

**引理 7** 命 $r_1,r_2$ 与 $r_3$ 为最小的三个正素数, 它们都是 mod $p$ 的二次非剩余. 则

$$r_1\leqslant p^{\frac{1}{2}},\quad r_2\leqslant\frac{2}{1-\frac{1}{r_1}}p^{1/2},\quad r_3\leqslant\frac{4}{\left(1-\frac{1}{r_1}\right)\left(1-\frac{1}{r_2}\right)}p^{\frac{1}{2}}.$$

**证明** 由引理 5 立即得到第一个不等式②, 否则取 $A=p^{\frac{1}{2}}$. 则

$$\frac{1}{2}p\geqslant\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right)=\sum_{a=1}^{A}\sum_{n=1}^{a}1=\sum_{a=1}^{A}a=\frac{1}{2}A(A+1).$$

这是不可能的.

由引理 6, 取 $A=r_{2-1}$, 我们得

$$\sum_{a=1}^{A}\sum_{n=1,(n,r_1)=1}^{a}1\leqslant Ap^{\frac{1}{2}}.$$

① $[x]$ 表示 $x$ 的整数部分.

② 见 A. Brauer. Über den kleinsten quadratischen Nichtrest. *Math. Zeit.*, 1931, 33: 161–176.

从而

$$\left(1-\frac{1}{r_1}\right)\sum_{a=1}^{A} a \leqslant Ap^{\frac{1}{2}},$$

即

$$(1-1/r_1)A(A+1)/2 \leqq Ap^{\frac{1}{2}}, \quad r_2 \leqslant \frac{2}{1-1/r_1}p^{\frac{1}{2}}.$$

由于

$$\left[\frac{a}{r_1}\right]+\left[\frac{a}{r_2}\right]-\left[\frac{a}{r_1r_2}\right] \leqslant \frac{a}{r_1}+\frac{a}{r_2}-\frac{a}{r_1r_2}.$$

所以类似地, 我们得第三个不等式.

## 5. 最小二次非剩余的增长性

**引理 8** (Vinogradov)① 命 $q_1,\cdots,q_s$ 为不超过 $A$ 的所有素数, 它们均为 $\bmod p$ 的二次非剩余. 则

$$\frac{1}{2}\sum_{n=1}^{A}\left(1-\left(\frac{n}{p}\right)\right)-\frac{1}{2}\sum_{n=1,(n,p)\neq 1}^{A} 1 \leqslant \sum_{\nu=1}^{s}\left(\frac{A}{q_\nu}\right).$$

**证明** 不等式的左端为不超过 $A$ 的非剩余 $n$ 的个数. 显然, 每一个这种 $n$ 皆可被 $q_s'$ 中的一个整除.

**引理 9** 在引理 8 的假定之下, 我们有

$$\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1}^{a}\left(1-\left(\frac{n}{p}\right)\right)-\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1}^{a} 1 \leqslant \sum_{a=1}^{A}\sum_{q_1\leqslant q_\nu\leqslant a}\left[\frac{a}{q_\nu}\right].$$

**证明** 将引理 7 中的公式加起来即得引理.

**引理 10** 我们有

$$\sum_{q_1\leqslant q\leqslant A}\left[\frac{A}{q}\right]=\sum_{\nu=1}^{[A/q_1]}\pi\left(\frac{A}{\nu}\right)-\left[\frac{A}{q_1}\right](\pi(q_1)-1),$$

此处 $q$ 过适合不等式

$$q_1 \leqslant q \leqslant A$$

的所有素数.

① *Trans. Amer. Math. Soc.*, 1927, 29: 216–226.

**证明** 我们有

$$\begin{aligned}\sum_{q_1\leqslant q\leqslant A}\left[\frac{A}{q}\right]&=\sum_{A\geqslant q>A/2}1+\sum_{A/2\geqslant q>A/3}2+\cdots+\sum_{A/[A/q_1]\geqslant q\geqslant q_1}\left[\frac{A}{q_1}\right]\\&=\pi(A)-\pi(A/2)+2\pi(A/2)-\pi(A/3)+\cdots\\&\quad+\left[\frac{A}{q_1}\right]\left(\pi\left(A\Big/\left[\frac{A}{q_1}\right]\right)-\pi(q_1)+1\right)\\&=\sum_{\nu=1}^{[A/q_1]}\pi\left(\frac{A}{\nu_1}\right)-\left[\frac{A}{q_1}\right](\pi(q_1)-1).\end{aligned}$$

**引理 11** 当 $q<A$ 时, 我们有

$$\sum_{a=1}^{A}\sum_{\nu=1}^{[a/q]}\pi\left(\frac{a}{\nu}\right)<1.0376\times A(A+1)/2\left(\log\frac{\log A}{\log q}+\frac{\mathrm{li}q}{q}+\frac{1.85}{q}\right).$$

**证明** 当 $q<a<A$ 时, 由引理 2 与引理 4 得

$$\begin{aligned}\sum_{\nu=1}^{a/q}\pi\left(\frac{a}{\nu}\right)&<1.0376\sum_{\nu=1}^{q/q}\left(\mathrm{li}\frac{a}{\nu}+1.85\right)\\&<1.0376\left(a\log\frac{\log a}{\log q}+\frac{a}{q}\mathrm{li}q+1.85\frac{a}{q}\right)\\&<1.0376\left(a\log\frac{\log A}{\log q}+a\frac{\mathrm{li}q}{q}+1.85\frac{a}{q}\right).\end{aligned}$$

当 $q>a$ 时, 这一不等式显然成立, 所以

$$\sum_{a=1}^{A}\sum_{\nu=1}^{a/q}\pi\left(\frac{a}{\nu}\right)<\frac{1.0376}{2}A(A+1)\left(\log\frac{\log A}{\log q}+\frac{\mathrm{li}q}{q}+\frac{1.85}{q}\right).$$

**定理 1** 命 $q_1$ 为最小二次非剩余, mod $p$. 则当 $p>\mathrm{e}^{250}$ 时有

$$q_1\leqslant(60p^{\frac{1}{2}})^{0.625}.$$

**证明** (1) 当 $q_1\leqslant\mathrm{e}^{80}$ 时, 我们有

$$q_1<(60\mathrm{e}^{125})^{0.625}\leqslant(60p^{\frac{1}{2}})^{0.625}.$$

(2) 我们假定 $q_1>\mathrm{e}^{80}$, 则由引理 9, 引理 10 与引理 11 得

$$\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1}^{a}\left(1-\left(\frac{n}{p}\right)\right)\leqslant\sum_{a=1}^{A}\sum_{q_1\leqslant q\leqslant a}\left[\frac{a}{q}\right]$$

$$= \sum_{a=1}^{A} \sum_{\nu=1}^{[a/q_1]} \pi\left(\frac{a}{\nu}\right) - \sum_{a=1}^{A} \left[\frac{a}{q_1}\right] (\pi(q_1) - 1)$$
$$< 1.0376 \frac{A(A+1)}{2} \left(\log \frac{\log A}{\log q_1} + \frac{\mathrm{li} q_1}{q_1} + \frac{1.85}{q_1}\right)$$
$$- \frac{A(A+1)}{2} \left(\frac{1}{q_1} - \frac{2}{A+1}\right) (\pi(q_1) - 1).$$

由引理 5 与引理 2 可知

$$\frac{1}{2}\left(\frac{A(A+1)}{2} - \frac{Ap^{\frac{1}{2}}}{2}\right)$$
$$< 1.0376 \frac{A(A+1)}{2} \left(\log \frac{\log A}{\log q_1} + \frac{\mathrm{li} q_1}{q_1} + \frac{1.85}{q_1}\right)$$
$$- \frac{A(A+1)}{2} \left(\frac{1}{q_1} - \frac{2}{A+1}\right) (0.9607\, \mathrm{li} q_1 - 2.7).$$

所以

$$\log\log q_1 < \log\log A + \frac{\mathrm{li} q_1}{q_1} + \frac{1.85}{q_1}$$
$$- \frac{1}{1.0376}\left(\frac{1}{2} - \frac{p^{1/2}}{2(A+1)}\right)$$
$$- \frac{1}{1.0376}\left(\frac{1}{q_1} - \frac{2}{A+1}\right)(0.9607 \mathrm{li} q_1 - 2.7).$$

取

$$A + 1 = 60 p^{\frac{1}{2}},$$

易得

$$\log\log q_1 < \log\log A + 0.07412 \mathrm{li} q_1/q_1 + 4.453/q_1$$
$$- 0.48188 + 0.00804$$
$$+ 0.03115 \mathrm{li} q_1/p^{\frac{1}{2}} - 0.0546(1/p^{\frac{1}{2}}).$$

所以

$$\log\log q_1 < \log\log A - 0.472$$

对于 $e^{80} < q_1 < p^{\frac{1}{2}}$ 及

$$0.07412 \mathrm{li} q_1/q_1 < 0.07412 \mathrm{li} e^{80}/e^{80} < 0.00095,$$

$$4.453/q_1 < 10^{-33},$$

$$0.03115 \mathrm{li} q_1/p^{\frac{1}{2}} < 0.03115 \mathrm{li} p^{\frac{1}{2}}/p^{\frac{1}{2}} < 0.03115/38 = 0.00082$$

成立. 因此

$$q_1 < A^{e^{-0.472}} < A^{0.625}.$$

我们还有

**定理 2** 命 $q_1, q_2$ 与 $q_3$ 为三个素数二次非剩余 $\bmod p$, 则当 $p \geqslant e^{250}$ 时有

$$q_2 \leqslant (240p^{1/2})^{0.625}$$

及

$$q_3 \leqslant (720p^{1/2})^{0.625}.$$

定理 2 的证明与定理 1 的证明是类似的, 但我们需分别从不等式

$$\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1, q_1\nmid n}^{a}\left(1-\left(\frac{n}{p}\right)\right) \leqslant \sum_{a=1}^{A}\left(\sum_{q_2\leqslant q\leqslant a}\left[\frac{a}{q}\right] - \sum_{q_2\leqslant q\leqslant a/q_1}\left[\frac{a}{q_1 q}\right]\right)$$

与

$$\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1, (q_1q_2, n)=1}^{a}\left(1-\left(\frac{n}{p}\right)\right) \leqslant \sum_{a=1}^{A}\left(\sum_{q_3\leqslant q\leqslant a}\left[\frac{a}{q}\right] - \sum_{q_3\leqslant q\leqslant a/q_1}\left[\frac{a}{q_1 q}\right] - \sum_{q_3\leqslant q\leqslant a/q_2}\left[\frac{a}{q_2 q}\right] - \sum_{q_3\leqslant q\leqslant a/q_1q_2}\left[\frac{a}{q_1 q_2 q}\right]\right)$$

开始, 来代替不等式

$$\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1}^{a}\left(1-\left(\frac{n}{p}\right)\right) \leqslant \sum_{a=1}^{A}\sum_{q_1\leqslant q\leqslant a}\left[\frac{a}{q}\right].$$

其对应的估计由引理 6 给出.

## 6. 二次域 E. A. 存在性的一个必要条件

**引理 12**① 对于一个形如 $4n+1$ 的素数 $p$, 若 $p$ 可以写成形式

$$p = q_1 n_1 + q_2 n_2,$$

此处 $n_1, n_2, q_1, q_2$ 皆为正的二次非剩余 $(\bmod p)$, 及当 $i = 1, 2$ 时, $q_1$ 为奇素数, 它整除 $q_i n_i$ 至一个奇数幂, 则在 $R(p^{1/2})$ 中不存在 E.A.

**引理 13** 假定 $s < q_1$. 命 $p_0$ 为不能整除 $s$ 的最小素数, 则

$$p_0 \leqslant (1/0.346)\log q_1.$$

① P. Erdös and Ch. Ko. Note on the Euclidean algorithm. *J. London Math. Soc.*, 1938, 13: 3–8.

**证明** 由引理 3 可知

$$\vartheta((1/0.346)\log q_1) \geqslant \log q_1 > \log s.$$

所以存在一个素数，不超过 $(1/0.346)\log q_1$，且不能整除 $s$.

**引理 14** 命 $p$ 为形如 $4n+1$ 的一个素数. 命 $q_1, q_2$ 与 $q_3$ 为三个最小的素数二次非剩余 mod $p$. 假定 $q_1 > 3$，若

$$p > (1/0.346)q_1q_2q_3\log q_1,$$

则我们可以找到两个整数 $s$ 与 $t$ 使

$$p = sq_2q_3 + tq_1,$$

此处 $\left(\frac{s}{p}\right) = 1$ 及 $(s, q_2q_3) = (t, q_1) = 1$.

**证明** 我们有

$$p = sq_2q_3 + tq_1, \quad 0 < s < q_1.$$

若 $q_1 \nmid t$，则由于

$$sq_2q_3 < q_1q_2q_3 < p.$$

所以由引理 12 即得引理. 其他条件显然成立.

若 $q_1|t$，命 $p_0$ 为不能整除 $s$ 的最小素数，则存在一个整数 $\mu$ 使

$$s + \mu q_1 \equiv 0(\mathrm{mod} p_0), \quad 0 < \mu < p_0 < q_1.$$

所以

$$p = ((s + \mu q_1)/p_0)p_0q_2q_3 + (t - \mu q_2q_3)q_1.$$

由于

$$s + \mu q_1/p_0 < (1 + \mu)q_1/p_0 \leqslant q_1$$

及由引理 13 可知

$$((s + \mu q_1)/p_0)p_0q_2q_3 < p_0q_1q_2q_3 < p,$$

所以由引理 12 即得引理.

**引理 15** 若 $q_1 > 3$ 及

$$(1/0.346)q_1q_2q_3\log q_1 < p,$$

则在 $R(p^{\frac{1}{2}})$ 中无 E. A.

**证明** 这一引理是引理 14 的推论.

**引理 16** 若 $q_1 = 3$，假定

$$5q_2q_3 < p, \quad 当 \left(\frac{5}{p}\right) = 1$$

与

$$40q_3 < p, \quad \text{当} \left(\frac{5}{p}\right) = -1.$$

则在 $R(p^{\frac{1}{2}})$ 中没有 E. A. 从而引理 15 对于 $q_1 = 3$ 亦成立.

**证明** (1) $\left(\frac{5}{p}\right) = 1$, 我们可以将 $p$ 写作

$$p = sq_2q_3 + 3t, \quad \text{此处 } s = 1 \text{ 或 } 2.$$

若 $3 \nmid t$, 则这给予了我们一个所要求的分解; 若 $3|t$, 则

$$p = (s+3)q_2q_3 + 3(t - q_2q_3),$$

将给我们同样的结果

(2) $\left(\frac{5}{p}\right) = -1$, 则我们可以将 $p$ 写作

$$p = 5sq_3 + 3t, \quad \text{此处 } s = 1 \text{ 或 } 2.$$

当 $s = 1$ 时, (1) 中的方法给予了我们一个所要求的分解. 若 $s = 2$ 及 $3|t$, 记

$$p = 40q_3 + 3(t - 10q_3).$$

## 7. 证明定理中的 E.A. 部分

**定理 3** 当 $d > \mathrm{e}^{250}$ 为平方自由数时, 则在二次域 $R(p^{\frac{1}{2}})$ 中没有 E.A.

**证明** 按照已知结果, 我们只要考虑情况 $d = p \equiv 1 \pmod 4$ 即可. 由定理 3 知

$$(1/0.346)q_1q_2q_3 \log q_1 < (1/0.346)(60 \cdot 240 \cdot 720p^{3/2})^{0.625} \log(60p^{\frac{1}{2}})^{0.625} < p.$$

故由引理 15 和引理 16 即得定理.

(王元　译)

# 关于二次非剩余的分布及实二次域中的欧几里得算法 (II)[①]

华罗庚　闵嗣鹤 (昆明, 国立清华大学)

## 1. 导　　言

本文的目的为证明下面结果[②]:

假定 $p = 17 \pmod{24}$, 则除了解 $p = 17, 41, 89, 113$ 与 137 之外, 在 $R(p^{1/2})$ 中皆没有 E. A.

熟知当 $p = 17, 41$ 时, $R(p^{1/2})$ 为欧氏域, 所以有疑义的域仅为 $p = 89$, 113 及 137.

本文所用的方法为前文方法的精密化: 引用 Euler 求和公式及特征和的一个新估计.

定理与引理的编号仍延续文 I 的编号. 文 I 的记号在此每均予保留, 例如 $p$ 表示素数, $[\xi]$ 表示 $\xi$ 的整数部分, 及 $q_1 < q_2 < q_3$ 表示最小的三个素数二次非剩余, mod $p$.

## 2. 与素数有关的引理

**引理 17**　当 $11 \leqslant x \leqslant 10^6$ 时,

$$\mathrm{li}x - \mathrm{li}x^{1/2} < \pi(x) < \mathrm{li}x$$

(见 Rosser, 定理 1 与定理 3).

**引理 18**　当 $x \geqslant 400$ 时, $\vartheta(x) > (1 - 0.139)x$.

**证明**　当 $x < 10^6$ 时, 引用 Rosser 定理 7[③], 而当 $x > 10^6$ 时, 则用 Rosser 公式[④].

---

① 1943 年 11 月 29 日收到. 发表于 *Trans. Amer. Math. Soc.*, 1944, 56: 547-569.

② 编者注: 这里的证明与 L. Rédei 的证明是完全不同的. (见 Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörper. *Math. Ann.*, 1942, 118: 588-608. 在该文中, Rédei 证明了, 在二次域 $R(\mu^{1/2})$ 中, 当 $\mu > 41$ 且具有形式 $24n + 17$, 则 E. A. 不存在. 作者不知道这篇文章, 该杂志刚到中国.

③ 当 $0 < x \leqslant 10^6$ 时, $x - 2.78x^{1/2} < \vartheta(x)$.

④ 当 $x > \mathrm{e}^{13.8}$ 时, $\vartheta(x) > (1 - 0.0393)x$.

**引理 19**　当 $401 \leqslant a \leqslant b \leqslant a^2$ 时,

$$\sum_{a \leqslant q \leqslant b} \frac{1}{q^2} < \frac{1.2142}{a \log a},$$

此处 $q$ 过素数.

**证明**　由引理 1(见 I ) 与引理 18 得

$$\begin{aligned}
\sum_{a \leqslant q \leqslant b} \frac{1}{q^2} &\leqslant \sum_{a \leqslant n \leqslant b} \frac{\vartheta(n) - \vartheta(n-1)}{n^2 \log n} \\
&= \sum_{a \leqslant n \leqslant b} \vartheta(n) \left( \frac{1}{n^2 \log n} - \frac{1}{(n+1)^2 \log(n+1)} \right) \\
&\quad + \frac{\vartheta(b)}{(b+1)^2 \log(b+1)} - \frac{\vartheta(a-1)}{a^2 \log a} \\
&< 1.0376 \left( \sum_{a \leqslant n \leqslant b} n \left( \frac{1}{n^2 \log n} - \frac{1}{(n+1)^2 \log(n+1)} \right) \right. \\
&\quad \left. + \frac{b}{(b+1) n^2 \log(b+1)} \right) - \frac{(1-0.139)(a-1)}{a^2 \log a} \\
&= 1.0376 \sum_{a \leqslant n \leqslant b} \frac{1}{n^2 \log n} + \frac{0.1766(a-1)}{a^2 \log a} \\
&< \frac{1.0376}{\log a} \left( \frac{1}{a} - \frac{1}{b} + \frac{1}{a^2} \right) + \frac{0.1766}{a \log a} < \frac{1.2142}{a \log a}.
\end{aligned}$$

## 3. 关于三角和的一些结果

**引理 20**　若 $A$ 是一个不小于 1 的整数, $0 < y \leqslant \pi/2A$, 及 $|x| \leqslant 1$, 则

$$\left| \sum_{n=1}^{A} (-1)^n \frac{\sin xyn}{\sin yn} \right| \leqslant 1.$$

**证明**　不失一般性, 我们可以假定 $x > 0$. 当 $0 < z \leqslant \pi/2$ 时, 函数 $\sin xz / \sin z$ 是递增的. 事实上

$$\frac{\mathrm{d}}{\mathrm{d}z} \frac{\sin xz}{\sin z} = \frac{x \sin z \cos xz - \cos z \sin xz}{\sin^2 z} \geqslant 0,$$

这是由于当 $z = 0$ 时, 上面表达式的分子为 0, 而当 $0 < z \leqslant \pi/2$ 时, 表达式的分子的微商 $(1 - x^2) \sin z \sin xz \geqslant 0$.

因此引理所示的和为一个交错级数, 并有绝对值递增项. 由于 $0 < x \leqslant 1$ 及 $0 < yn \leqslant \pi/2$, 所以

$$0 < \sin xyn / \sin yn \leqslant 1.$$

引理证完.

**引理 21** 命 $A$ 为一个不小于 1 的整数及 $m$ 为一个不超过 $p/2A$ 的正整数, 及命

$$S_m = S_m(A) = 2\sum_{x=1}^{[(p-1)/2m]}\left(\frac{\sin\pi(A+1)mx/p}{\sin\pi mx/p}\right)^2.$$

则

$$|S_m - p(A+1)/m + (A+1)^2| < 3A+1$$

与

$$S_1 = p(A+1) - (A+1)^2.$$

**证明** 为简单起见, 记

$$e(x) = \mathrm{e}^{2\pi ix}.$$

我们并用 $Rx$ 表示 $x$ 的实数部分, 则得

$$\begin{aligned}
S_m &= 2\sum_{x=1}^{[(p-1)/2m]}\sum_{a=0}^{A}\sum_{n=-a}^{a} e(mnx/p)\\
&= 2\left[\frac{p-1}{2m}\right](A+1) + 4\sum_{a=1}^{A}\sum_{n=1}^{a} R\left(\frac{\begin{array}{c}2e(mn/p)([(p-1)/2m]+1/2))\\ -e(mn/2p)+e(-mn/2p)\end{array}}{\begin{array}{c}2(e(mn/2p)\\ -e(-mn/2p))\end{array}}\right)\\
&= 2\left[\frac{p-1}{2m}\right](A+1) - A(A+1)\\
&\quad + 4\sum_{a=1}^{A}\sum_{n=1}^{a} R\frac{e((mn/p)([(p-1)/2m]+1/2))}{e(mn/2p)-e(-mn/2p)}\\
&= 2\left[\frac{p-1}{2m}\right](A+1) - A(A+1)\\
&\quad + 2\sum_{a=1}^{A}\sum_{n=1}^{a}\frac{\sin([(p-1)/2m]+1/2)2\pi mn/p}{\sin\pi mn/p}\\
&= 2\left[\frac{p-1}{2m}\right](A+1) - A(A+1)\\
&\quad + 2\sum_{a=1}^{A}\sum_{n=1}^{a}(-1)^n\frac{\sin([(p-1)/2m]-p/2m+1/2)2\pi mn/p}{\sin\pi mn/p}\\
&= 2\left[\frac{p-1}{2m}\right](A+1) - A(A+1) + 2A\theta,
\end{aligned}$$

此处 $|\theta| \leqslant 1$, 并用到引理 20, 其中 $m \leqslant p/2A \leqslant p/2a$ 及 $-1+1/2m \leqslant [(p-1)/2m]-(p-1)/2m \leqslant 0$.

由于

$$\begin{aligned}-2(A+1) &\leqslant 2[(p-1)/2m](A+1)-p(A+1)/m\\ &\leqslant -(A+1)/m<0,\end{aligned}$$

所以

$$-4A-2<S_m-p(A+1)/m+A(A+1)<2A.$$

故得引理所示的不等式.

特别当 $m=1$ 时有 $\vartheta=0$, 故等式成立.

**引理 22** 当 $\alpha \geqslant 0$ 时有

$$\sum_{n=1}^{\infty}\frac{\sin^2\pi n\alpha}{n^2}=\frac{\pi^2}{2}(\{\alpha\}-\{\alpha\}^2),$$

此处 $\{\alpha\}=\alpha-[\alpha]$ (见, 例如, Wittaker-Watson. *Modern Analysis*, 4th ed, Example 3, p. 163.)

**引理 23** 命 $A \geqslant 0, m>0$, 则

$$-\frac{4p}{\pi^2 m}-\frac{8}{\pi^2}<S_m-\frac{p^2}{m^2}\left(\left\{\frac{(A+1)m}{p}\right\}-\left\{\frac{(A+1)m}{p}\right\}^2\right)<\frac{5p}{6m}.$$

**证明** (1) 当 $0 \leqslant x \leqslant \pi/2$ 时, $\sin x \leqslant x$. 由于

$$[(p-1)/2m]+1>(p-1)/2m-(2m-1)/2m+1=p/2m$$

与

$$\sum_{x=[(p-1)/2m]+1}^{\infty}\frac{1}{x^2}<\int_{p/2m}^{\infty}\frac{\mathrm{d}x}{x^2}+\frac{4m^2}{p^2}=\frac{2m}{p}+\frac{4m^2}{p^2}.$$

所以

$$\begin{aligned}S_m &> 2\sum_{x=1}^{[(p-1)/2m]}\frac{\sin^2\pi(A+1)mx/p}{(\pi mx/p)^2}\\ &> \frac{2p^2}{\pi^2m^2}\left(\sum_{x=1}^{\infty}\frac{\sin^2\pi(A+1)mx/p}{x^2}-\sum_{x=[(p-1)/2m]+1}^{\infty}\frac{1}{x^2}\right)\\ &> \frac{2p^2}{\pi^2m^2}\left(\sum_{x=1}^{\infty}\frac{\sin^2\pi(A+1)mx/p}{x^2}-\frac{2m}{p}-\frac{4m^2}{p^2}\right),\end{aligned}$$

由引理 22 可知

$$S_m>\frac{p^2}{m^2}\left(\left\{\frac{(A+1)m}{p}\right\}-\left\{\frac{(A+1)m}{p}\right\}^2\right)-\frac{4p}{\pi^2 m}-\frac{8}{\pi^2}.$$

(2) 当 $0 \leqslant x \leqslant 0.44$ 时, 我们有

$$(1-x)^{-2} \leqslant 1+5x,$$

而当 $0 < x \leqslant \pi/2$ 时, 我们有

$$\sin x > x - x^3/6.$$

所以当 $1 < x \leqslant (p-1)/2m$ 时,

$$\begin{aligned}\frac{1}{(\sin \pi mx/p)^2} &< \frac{1}{(\pi^2 m^2 x^2/p^2)(1-\pi^2 m^2 x^2/6p^2)^2} \\ &< \frac{p^2}{\pi^2 m^2 x^2}\left(1+\frac{5\pi^2 m^2 x^2}{6p^2}\right),\end{aligned}$$

其中用到

$$\pi^2 m^2 x^2/6p^2 < \pi^2/24 < 0.44.$$

因此由引理 22 得

$$\begin{aligned}S_m &< 2\sum_{x=1}^{[(p-1)/2m]} \frac{p^2}{\pi^2 m^2} \frac{\sin^2 \pi(A+1)mx/p}{x^2}\left(1+\frac{5\pi^2 m^2 x^2}{6p^2}\right) \\ &< \frac{2p^2}{\pi^2 m^2}\left(\sum_{x=1}^{\infty} \frac{\sin^2 \pi(A+1)mx/p}{x^2} + \sum_{x=1}^{[(p-1)/2m]} \frac{5\pi^2 m^2}{6p^2}\right) \\ &< \frac{p^2}{m^2}\left(\left\{\frac{(A+1)m}{p}\right\} - \left\{\frac{(A+1)m}{p}\right\}^2\right) + \frac{5p}{6m}.\end{aligned}$$

## 4. 与特征和有关的结果

**引理 24** 命 $p > 10^6$ 及

$$N = N(A) = 2\sum_{x=1}^{(p-1)/2}{}' \left(\frac{\sin \pi(A+1)x/p}{\sin \pi x/p}\right)^2,$$

此处 $\sum'$ 表示过二次非剩余 mod $p$ 求和. 若 $q_1 = 3, q_2 > p^{1/2}/37.5, q_3 \geqslant (p/5)^{1/2}$, 则当 $1 \leqslant A < 10p^{1/2}$ 时有

$$N > 20p(A+1)/81 - 0.05314pp^{1/2}.$$

**证明** 由于所有小于 $3(p/5)^{1/2}$ 的正整数, 它们不能被 $q_2$ 整除, 但却好被 3 或 $3^3 = 27$ 整除者为二次非剩余, mod $p$. 所以

$$N > (S_3 - S_9) + (S_{27} - S_{81}) - S_{3q_2} - \sum_{(p/5)^{1/2} \leqslant q \leqslant (p-1)/6} S_{3q},$$

此处 $q$ 过素数.

由于 $2A \times 27 < 540p^{1/2} < p$, 所以由引理 21 得

$$S_3 - S_9 + S_{27} > (1/3 - 1/9 + 1/27)p(A+1) - (A+1)^2 - 9A - 3$$
$$= (7/27)p(A+1) - (A+1)^2 - 9A - 3. \tag{1}$$

由于 $81(A+1) < 810(p^{1/2}+1) < p$, 所以由引理 23 得

$$S_{81} < p(A+1)/81 - (A+1)^2 + 5p/486. \tag{2}$$

由于对于所有的 $x$ 皆有 $\{x\} - \{x\}^2 \leqslant \frac{1}{4}$, 所以由同一引理得

$$S_{3q_2} < \frac{p^2}{9q_2^2} \times \frac{1}{4} + \frac{5p}{18q_2} = \frac{p^2}{36q_2^2} + \frac{5p}{18q_2} < 0.03909pp^{1/2}, \tag{3}$$

类似地, 由引理 19 得

$$\sum_{(p/5)^{1/2} \leqslant q \leqslant (p-1)/6} S_{3q} < \sum_{(p/5)^{1/2} \leqslant q \leqslant (p-1)/6} \left(\frac{p^2}{36q^2} + \frac{5p}{18q}\right)$$
$$< \frac{p^2}{36} \frac{1.2142}{(p/5)^{1/2}\log(p/5)^{1/2}} + \frac{5p}{18}\left(\log\frac{(5p)^{1/2}}{6} + \left(\frac{5}{p}\right)^{1/2}\right),$$

所以

$$\sum_{(p/5)^{1/2} \leqslant q \leqslant (p-1)/6} S_{3q} < \frac{1.2142(5)^{1/2}}{36 \times 6.103} pp^{1/2} + \frac{5pp^{1/2}}{18000}(5.9208 + 0.0023)$$
$$= \frac{2.71508}{219.708} pp^{1/2} + \frac{5 \times 5.9231}{18000} pp^{1/2}$$
$$= (0.01236 + 0.00165)pp^{1/2}$$
$$= 0.01401pp^{1/2}. \tag{4}$$

由 (1), (2), (3) 与 (4) 得

$$N > 20p(A+1)/81 - 9A - 3 - 5p/486 - (0.03909 + 0.01401)pp^{1/2}$$
$$> 20p(A+1)/81 - 9A - 3 - 0.00002pp^{1/2} - 0.0531)pp^{1/2}$$
$$> 20p(A+1)/81 - 0.05314pp^{1/2}.$$

**引理 25**　命 $p \equiv 1 \pmod 4$ 及

$$S = \sum_{a=1}^{A} \sum_{n=1, 3 \nmid n}^{a} \left(\frac{n}{p}\right).$$

则在引理 24 的条件下, 当 $p^{1/2} < A < 10p^{1/2}$ 时有

$$S < 41Ap^{1/2}/81 + 0.21256p.$$

**证明** 我们有

$$\begin{aligned} S &= \sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right) + \sum_{a=1}^{A}\sum_{n=1}^{[a/3]}\left(\frac{n}{p}\right) \\ &\leqslant \sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right) + 2\sum_{a=1}^{[\frac{A}{3}-1]}\sum_{n=1}^{a}\left(\frac{n}{p}\right) + 3\left|\sum_{n=1}^{[A/3]}\left(\frac{n}{p}\right)\right|. \end{aligned}$$

如 I, 引理 5 之证明所示得

$$\begin{aligned} p^{1/2}\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{n}{p}\right) &= \sum_{x=1}^{(p-1)/2}\left(\frac{x}{p}\right)\left(\frac{\sin x(A+1)x/p}{\sin \pi x/p}\right)^2 \\ &= S_1(A)/2 - N(A). \end{aligned}$$

所以由引理 21 与引理 24 得

$$\begin{aligned} S &\leqslant \frac{1}{2p^{1/2}}S_1(A) - \frac{1}{p^{1/2}}N(A) + \frac{3}{2p^{1/2}}S_1\left(\left[\frac{A}{3}-1\right]\right) \\ &\quad - \frac{3}{p^{1/2}}N\left(\left[\frac{A}{3}-1\right]\right) + A \\ &< \frac{1}{2p^{1/2}}\left(p(A+1) - (A+1)^2 - \frac{40}{81}p(A+1) + 0.10628pp^{1/2}\right) \\ &\quad + \frac{3}{2p^{1/2}}\left(p\left[\frac{A}{3}\right] - \left[\frac{A}{3}\right]^2 - \frac{40}{81}p\left[\frac{A}{3}\right] + 0.10628pp^{1/2}\right) + A \\ &< \frac{1}{2p^{1/2}}\left(\frac{41}{81}p(A+1) - (A+1)^2 + 0.10628pp^{1/2}\right) \\ &\quad + \frac{3}{2p^{1/2}}\left(\frac{41}{81}p\frac{A}{3} + 0.10628pp^{1/2}\right) < \frac{41}{81}Ap^{1/2} + 0.21256p. \end{aligned}$$

**引理 26** 命 $p \equiv 1 \pmod 4$, 则在引理 24 的条件下得

$$q_3 < 3p^{1/2}.$$

**证明** 当 $A < q_3$ 时有

$$\begin{aligned} \sum_{a=1}^{A}\sum_{n=1,3\nmid n}^{a}\left(\frac{n}{p}\right) &> \sum_{a=1}^{A}\sum_{n=1,3\nmid n}^{a}1 - \sum_{a=1}^{A}\sum_{n=1,q_2|n}^{a}1 + \sum_{a=1}^{A}\sum_{n=1,3q_2|n}^{a}1 \\ &> A(A+1)/3 - (1/3q_2)A(A+1) - 2A. \end{aligned}$$

由 I, 引理 7 可知 $q_3 < 7.5p^{1/2} < 10p^{1/2}$, 所以当 $A = q_3 - 1$ 时, 由引理 25(若 $A < p^{1/2}$. 则结果显然成立) 得

$$(A(A+1)/3)(1-1/q_2) - 2A < 41Ap^{1/2}/81 + 0.21256p,$$
$$(A(A+1)/3)(1-0.0375) - 2A < 0.5062Ap^{1/2} + 0.21256p,$$
$$0.3208A^2 - 1.6792A < 0.5062Ap^{1/2} + 0.21256p,$$
$$0.3208A^2 - 0.5079Ap^{1/2} - 0.21256p < 0.$$

所以

$$A < (1/0.6414)(0.5079 + (0.5079^2 + 4 \times 0.3208 \times 0.21256)^{1/2})p^{1/2},$$

从而

$$q_3 < 3p^{1/2}.$$

## 5. 关于和的一些引理

**引理 27**　当 $q > 0$ 时, 我们有

$$\frac{(A+2)(A-q)}{2q} < \sum_{a=1}^{A}\left[\frac{a}{q}\right] < \frac{1}{29}\left(A - \frac{(q-2)}{2}\right)^2.$$

**证明**　我们有

$$\begin{aligned}\sum_{a=1}^{A}\left[\frac{a}{q}\right] &= \sum_{q\leqslant a<2q} + \sum_{2q\leqslant a<3q} + \cdots + \sum_{([A/q]-1)q\leqslant a<[A/q]q}\left[\frac{A}{q}-1\right] + \sum_{[A/q]q\leqslant a\leqslant A}\left[\frac{A}{q}\right]\\ &= q\left(1+2+\cdots+\left[\frac{A}{q}-1\right]\right) + \left(A - \left[\frac{A}{q}\right]q + 1\right)\left[\frac{A}{q}\right]\\ &= \frac{1}{2}q\left[\frac{A}{q}\right]\left(\left[\frac{A}{q}\right]-1\right) + \left(A - \left[\frac{A}{q}\right]q + 1\right)\left[\frac{A}{q}\right]\\ &= \frac{1}{2}\left[\frac{A}{q}\right]\left(2A + 2 - \left[\frac{A}{q}\right]q - q\right)\\ &= \frac{1}{2q}(A - \vartheta q)(A - q + \vartheta q + 2)\\ &= \frac{1}{2q}\left(\left(A - \frac{q}{2} + 1\right)^2 - \left(\vartheta q + 1 - \frac{q}{2}\right)^2\right), \quad \vartheta = \frac{A}{q} - \left[\frac{A}{q}\right],\end{aligned}$$

它介于 $(A+2)(A-q)/2q$ 与 $(A-q/2+1)^2/2q$ 之间.

**引理 28** (Euler 求和公式)　命 $b_1(x) = x - [x] - 1/2$ 及

$$b_2(x) = \frac{1}{12} + \int_0^x b_1(x)\mathrm{d}x.$$

命 $b>a$ 及 $g(x)$ 在 $a\leqslant x<b$ 中有连续二阶微商. 则

$$\sum_{a\leqslant m<b} g(m)=\int_a^b g(x)\mathrm{d}x+g(b)b_1(-b)-g(a)b_1(-a)$$
$$+g'(b)b_2(-b)-g'(a)b_2(-a)$$
$$-\int_a^b g''(x)b_2(-x)\mathrm{d}x.$$

**引理 29** 当 $a-\lambda q>3q\geqslant 9$ 时,

$$\sum_{\nu=1}^{[(a-\lambda q)/3q]}\mathrm{li}\frac{a}{3\nu+\lambda}<\frac{a}{3}\log\frac{\log(a/(3+\lambda))}{\log q}$$
$$+\frac{(3\lambda+10.7322)a}{12(3+\lambda)^3\log(a/(3+\lambda))}$$
$$-\frac{3q^2b_2(-(a-\lambda q)/3q)}{a\log q}+\frac{a}{3q}\mathrm{li}q$$
$$-\left(\frac{1}{2}+\frac{\lambda}{3}\right)\mathrm{li}\frac{a}{3+\lambda}+\mathrm{li}q b_1\left(-\frac{a-\lambda q}{3q}\right)+R,$$

此处按 $3q$ 能或不能整除 $a-\lambda q$ 而定 $R=\mathrm{li}q$ 或 0.

**证明** 命 $g(x)=\mathrm{li}a/(3x+\lambda)$, 则

$$g'(x)=-\frac{3a}{(3x+\lambda)^2\log(a/(3x+\lambda))},$$

$$g''(x)=\frac{9a(2\log(a/(3x+\lambda))-1)}{(3x+\lambda)^3\log^2(a/(3x+\lambda))},$$

及当 $1\leqslant 3x+\lambda\leqslant(1/\mathrm{e})a$ 时, 由于当 $u>1$ 时, $(2u-1)/u^2$ 为递减函数, 所以 $g''(x)$ 为递减函数.

由于

$$\int_1^{(a-\lambda q)/3q}\mathrm{li}\frac{a}{3t+\lambda}\mathrm{d}t=\frac{1}{3}\left((3t+\lambda)\mathrm{li}\frac{a}{3t+\lambda}\right)_1^{(a-\lambda q)/3q}$$
$$-\frac{a}{3}\int_1^{(a-\lambda q)/3q}\frac{d(a/(3t+\lambda))/\mathrm{d}t}{a/(3t+\lambda)\log(a/(3t+\lambda))}\mathrm{d}t$$
$$=\frac{1}{3}\left((3t+\lambda)\mathrm{li}\frac{a}{3t+\lambda}\right)_1^{(a-\lambda q)/3q}$$
$$-\frac{a}{3}\left(\log\log\frac{a}{3t+\lambda}\right)_1^{(a-\lambda q)/3q}$$

$$= \frac{a}{3q}\mathrm{li}q - \frac{1}{3}(3+\lambda)\mathrm{li}\frac{a}{3+\lambda} + \frac{a}{3}\log\frac{\log(a/(3+\lambda))}{\log q}$$

及

$$\left|\int_0^x b_2(-x)\mathrm{d}x\right| \leqslant \frac{3^{1/2}}{216}①.$$

所以由引理 28 可知

$$\sum_{\nu=1}^{[(a-\lambda q)/3q]} \mathrm{li}\frac{a}{3\nu+\lambda} = \int_1^{(a-\lambda q)/3q} \mathrm{li}\frac{a}{3t+\lambda}\mathrm{d}t + \frac{1}{2}\mathrm{li}\frac{a}{3+\lambda}$$
$$+ \mathrm{li}q b_1\left(-\frac{a-\lambda q}{3q}\right) + \frac{a}{4(3+\lambda)^2\log(a/(3+\lambda))}$$
$$- \frac{3ab_2(-(a-\lambda q)/3q)}{(a/q)^2\log q}$$

$$- \int_1^{(a-\lambda q)/3q} \frac{9a(2\log(a/(3x+\lambda))-1)b_2(-x)}{(3x+\lambda)^3\log^2(a/(3x+\lambda))}\mathrm{d}x + R$$
$$= \frac{a}{3}\log\frac{\log(a/(3+\lambda))}{\log q} + \frac{a}{3q}\mathrm{li}q - \frac{1}{3}(3+\lambda)\mathrm{li}\frac{a}{3+\lambda}$$
$$+ \frac{1}{2}\mathrm{li}\frac{a}{3+\lambda} + \mathrm{li}q b_1\left(-\frac{a-\lambda q}{3q}\right)$$
$$+ \frac{a}{4(3+\lambda)^2\log(3/(3+\lambda))} - \frac{3q^2b_2(-(a-\lambda q)/3q)}{a\log q}$$
$$+ \frac{3^{1/2}a\theta}{12(3+\lambda)^3\log(a/(3+\lambda))} + R,$$

此 $\theta \leqslant 1$, 引理证完.

**引理 30** 在条件 $\lambda > 0$ 及引理 29 的条件下, 我们有

$$\sum_{a=\lambda q}^{A} \sum_{\nu=0}^{[(a-\lambda q)/3q]} \mathrm{li}\frac{a}{3\nu+\lambda} < \frac{1}{6}A(A+2)\log\log\frac{A}{3+\lambda}$$
$$- \frac{1}{6}(A^2+A+(3+\lambda)q)\log\log q + (A+1)\mathrm{li}\frac{A}{\lambda}$$
$$- \frac{(2\lambda+3)A}{6}\mathrm{li}\frac{A}{3+\lambda}$$

---

① 当 $0 < x \leqslant 1$ 时, $\int_0^x b_2(-z)\mathrm{d}x = \int_0^x ((x^2-x)/2+1/12)\mathrm{d}x = (x/12)(2x^2-3x+1)$, 它在 $x = (3 \pm 3^{1/2})/6$ 时取极值. 当 $x = 1$ 时, 积分等于 0. 由于 $b_2(x-1) = b_2(x)$, 故得所要求的公式.

$$+\frac{\mathrm{li}q}{24q}(4A^2+8A+(2\lambda-3)^2q^2+4)$$
$$+\frac{3\lambda+10.7322}{12(\lambda+3)^3}\frac{A}{\log A/3(3+\lambda)}$$
$$+\frac{q^2}{8\log q}\left(\log\frac{A}{(3+\lambda)q}+\frac{1}{(3+\lambda)q}\right)-\lambda\int_q^{A/\lambda}\frac{x\mathrm{d}x}{\log x}$$
$$+\frac{2\lambda(3+\lambda)^2+3\lambda+10.7322}{12(3+\lambda)}\int_q^{A/(3+\lambda)}\frac{x\mathrm{d}x}{\log x}.$$

**证明** 由引理 29, 得

$$\sum_{a=\lambda q}^{A}\sum_{\nu=0}^{[(a-\lambda q)/3q]}\mathrm{li}\frac{a}{3\nu+\lambda}=\sum_{a=\lambda q}^{A}\mathrm{li}\frac{a}{\lambda}+\sum_{a=(3+\lambda)q}^{A}\sum_{\nu=1}^{[(a-\lambda q)/3q]}\mathrm{li}\frac{a}{3\nu+\lambda}$$
$$<\int_{\lambda q}^{A}\mathrm{li}\frac{x}{\lambda}\mathrm{d}x+\mathrm{li}\frac{A}{\lambda}+\sum_{a=(3+\lambda)q}^{A}\frac{a}{3}\log\frac{\log(a/(3+\lambda))}{\log q}$$
$$+\frac{3\lambda+10.7322}{12(3+\lambda)^3}\left(\int_{(3+\lambda)q}^{A}\frac{x\mathrm{d}x}{\log(x/(3+\lambda))}+\frac{A}{\log(A/(3+\lambda))}\right)$$
$$-\sum_{a=(3+\lambda)q}^{A}\frac{3q^2}{a\log q}b_2\left(-\frac{a-\lambda q}{3q}\right)$$
$$+\frac{1}{6q}(A+\lambda q+3q)(A-\lambda q-3q+1)\mathrm{li}q-\left(\frac{1}{2}+\frac{\lambda}{3}\right)$$
$$\cdot\int_{(3+\lambda)q}^{A}\mathrm{li}\frac{x}{3+\lambda}\mathrm{d}x+\mathrm{li}q\sum_{a=(3+\lambda)q}^{A}\left(b_1\left(-\frac{a-\lambda q}{3q}\right)+R'\right);$$

此处按 $3q$ 能整除或不能整除 $a-\lambda q$ 而定 $R'=1$ 或 0.

显然有

$$\int_{\lambda q}^{A}\mathrm{li}\frac{x}{\lambda}\mathrm{d}x=A\mathrm{li}\frac{A}{\lambda}-\lambda q\mathrm{li}q-\int_{\lambda/q}^{A}\frac{x\mathrm{d}x}{\lambda\log x/\lambda},$$

$$\sum_{a=(a+\lambda)q}^{A}\frac{a}{3}\log\log\frac{a}{3+\lambda}$$
$$<\frac{1}{3}\int_{(3+\lambda)q}^{A}x\log\log\frac{x}{3+\lambda}\mathrm{d}x+\frac{A}{3}\log\log\frac{A}{3+\lambda}$$
$$=\frac{1}{6}\left(A^2\log\log\frac{A}{3+\lambda}-(3+\lambda)^2q^2\log\log q\right)$$

$$+\frac{A}{3}\log\log\frac{A}{3+\lambda}-\frac{1}{6}\int_{(3+\lambda)q}^{A}\frac{x\mathrm{d}x}{\log x/(3+\lambda)}$$
$$-\sum_{a=(3+\lambda)q}^{A}\frac{b_2(-(a-\lambda q)/3q)}{a}<\frac{1}{24}\sum_{a=(3+\lambda)q}^{A}\frac{1}{a}$$
$$<\frac{1}{24}\left(\log\frac{A}{(3+\lambda)q}+\frac{1}{(3+\lambda)q}\right),$$

其中用到 $b_2(x)\geqslant -1/24$.

$$\int_{(3+\lambda)q}^{A}\mathrm{li}\frac{x}{3+\lambda}\mathrm{d}x=A\mathrm{li}\frac{A}{3+\lambda}-(3+\lambda)q\mathrm{li}q$$
$$-\int_{(3+\lambda)q}^{A}\frac{x\mathrm{d}x}{(3+\lambda)\log x/(3+\lambda)}$$

及

$$\sum_{a=(3+\lambda)q}^{A}\left(b_1\left(-\frac{a-\lambda q}{3q}\right)+R'\right)$$
$$=\sum_{n=0}^{A-(3+\lambda)q}\left(b_1\left(-\frac{n}{3q}\right)+R''\right)=S\ (\text{定义}).$$

此处按 $3q|n$ 或 $3q\nmid n$ 而定 $R''=1$ 或 0. 由于 $[-n/3q]=-[n/3q]+R''-1$, 所以

$$S=\sum_{n=0}^{A-(3+\lambda)q}\left(-\frac{n}{3q}-\left[-\frac{n}{3q}\right]-\frac{1}{2}+R''\right)$$
$$=\sum_{n=0}^{A-(3+\lambda)q}\left(-\frac{n}{3q}+f\left[-\frac{n}{3q}\right]+\frac{1}{2}\right),$$

由引理 27 可知

$$S<-\frac{1}{6q}(A-(3+\lambda)q)(A-(3+\lambda)q+1)$$
$$+\frac{1}{6q}\left(A-(3+\lambda)q-\frac{3q-2}{2}\right)^2+\frac{1}{2}(A-(3+\lambda)q+1)$$
$$=\frac{1}{6q}(A-\lambda q)+\frac{(3q-2)^2}{24q}.$$

所以

$$\sum_{a=\lambda q}^{A}\sum_{\nu=0}^{[(a-\lambda q)/3q]}\mathrm{li}\frac{q}{3\nu+\lambda}<A\mathrm{li}\frac{A}{\lambda}-\lambda q\mathrm{li}q-\int_{\lambda q}^{A}\frac{x\mathrm{d}x}{\lambda\log x/\lambda}+\mathrm{li}\frac{A}{\lambda}$$

$$
\begin{aligned}
&-\frac{1}{6}(A+\lambda q+3q)(A-\lambda q-3q+1)\log\log q\\
&+\frac{1}{6}\left(A^2\log\log\frac{A}{3+\lambda}-(3+\lambda)^2q^2\log\log q\right)+\frac{A}{3}\log\log\frac{A}{3+\lambda}\\
&-\frac{1}{6}\int_{(3+\lambda)q}^{A}\frac{x\mathrm{d}x}{\log x/(3+\lambda)}\\
&+\frac{3\lambda+10.7322}{12(3+\lambda)^3}\left(\int_{(3+\lambda)q}^{A}\frac{x\mathrm{d}x}{\log x/(3+\lambda)}+\frac{A}{\log A/(3+\lambda)}\right)\\
&+\frac{q^2}{8\log q}\left(\log\frac{A}{(3+\lambda)q}+\frac{1}{(3+\lambda)q}\right)\\
&+\frac{1}{6q}(A+\lambda q+3q)(A-\lambda q-3q+1)\mathrm{li}q\\
&-\left(\frac{1}{2}+\frac{\lambda}{3}\right)\left(A\mathrm{li}\frac{A}{3+\lambda}\right)-(3+\lambda)q\mathrm{li}q\\
&-\int_{(3+\lambda)q}^{A}\frac{x\mathrm{d}x}{(3+\lambda)\log x/(3+\lambda)}+\mathrm{li}q\left(\frac{A-\lambda q}{6q}+\frac{(3q-2)^2}{24q}\right)\\
=&\frac{1}{6}A(A+2)\log\log\frac{A}{3+\lambda}-\frac{1}{6}(A^2+A+(3+\lambda)q)\log\log q\\
&+(A+1)\mathrm{li}\frac{A}{\lambda}-\frac{2\lambda+3}{6}A\mathrm{li}\frac{A}{3+\lambda}+\frac{\mathrm{li}q}{24q}(4A^2+8A\\
&+(2\lambda-3)^2q^2+4)+\frac{3\lambda+10.7322}{12(3+\lambda)^3}\frac{A}{\log(A/(3+\lambda))}\\
&+\frac{q^2}{8\log q}\left(\log\frac{A}{(3+\lambda)q}+\frac{1}{(3+\lambda)q}\right)\\
&-\int_{\lambda q}^{A}\frac{x\mathrm{d}x}{\lambda\log x/\lambda}+\frac{2\lambda(3+\lambda)^2+3\lambda+10.7322}{12(3+\lambda)}\int_{q}^{A/(3+\lambda)}\frac{x\mathrm{d}x}{\log x}.
\end{aligned}
$$

**引理 31** 在引理 29 的条件下，

$$
\begin{aligned}
&\sum_{a=q}^{A}\left(\sum_{\nu=0}^{[(a-q)/3q]}\mathrm{li}\frac{a}{3\nu+1}+\sum_{\nu=0}^{[(a-2q)/3q]}\mathrm{li}\frac{a}{3\nu+2}\right)\\
<&\frac{1}{6}A(A+2)\log\left(\log\frac{A}{4}\log\frac{A}{5}\right)-\frac{1}{6}(2A^2+2A+9q)\log\log q\\
&+\frac{\mathrm{li}q}{12q}(4A^2+8A+q^2+4)+\frac{0.03A}{\log A/5}\\
&+\frac{q^2}{8\log q}\left(\log\frac{A^2}{20q^2}+\frac{q}{20q}\right)+A^2\left(\int_{1/2}^{A}\frac{(1-x)\mathrm{d}x}{\log Ax}\right.
\end{aligned}
$$

$$+\int_{1/4}^{1/2}\frac{(2-3x)\mathrm{d}x}{\log Ax}+\int_{1/5}^{1/4}\frac{(1.1667-2.0472x)\mathrm{d}x}{\log Ax}+0.1016\int_{q/A}^{1/5}\frac{x\mathrm{d}x}{\log Ax}\Bigg)$$

$$=\mathrm{li}A+\mathrm{li}\frac{A}{2}.$$

**证明** 由引理 30 可知问题中的和小于

$$\begin{aligned}
&\frac{1}{6}A(A+2)\log\left(\log\frac{A}{4}\log\frac{A}{5}\right)-\frac{1}{6}(2A^2+2A+9q)\log\log q\\
&+(A+1)\mathrm{li}A+(A+1)\mathrm{li}\frac{A}{2}-\frac{5}{6}A\mathrm{li}\frac{A}{4}-\frac{7}{6}A\mathrm{li}\frac{A}{5}\\
&+\frac{\mathrm{li}q}{12q}(4A^2+8A+q^2+4)+\frac{0.03A}{\log(A/5)}\\
&+\frac{q^2}{8\log q}\left(\log\frac{A^2}{20q^2}+\frac{9}{20q}\right)-\int_q^A\frac{x\mathrm{d}x}{\log x}-\int_{2q}^A\frac{x\mathrm{d}x}{2\log x/2}\\
=&\frac{45.7322}{48}\int_q^{A/4}\frac{x\mathrm{d}x}{\log x}+\frac{116.7322}{60}\int_q^{A/5}\frac{x\mathrm{d}x}{\log x}.
\end{aligned}$$

由于

$$\begin{aligned}
&A\mathrm{li}A+A\mathrm{li}\frac{A}{2}-\frac{5}{6}A\mathrm{li}\frac{A}{4}-\frac{7}{6}A\mathrm{li}\frac{A}{5}\\
=&A\int_{A/2}^{A}\frac{\mathrm{d}x}{\log x}+2A\int_{A/4}^{A/2}\frac{\mathrm{d}x}{\log x}+\frac{7}{6}A\int_{A/5}^{A/4}\frac{\mathrm{d}x}{\log x}
\end{aligned}$$

与

$$\begin{aligned}
&-\int_q^A\frac{x\mathrm{d}x}{\log x}-\int_{2q}^A\frac{x\mathrm{d}x}{2\log x/2}+\frac{45.7322}{48}\int_q^{A/4}\frac{x\mathrm{d}x}{\log x}\\
&+\frac{116.7322}{60}\int_q^{A/5}\frac{x\mathrm{d}x}{\log x}\\
=&-\int_{A/2}^{A}\frac{x\mathrm{d}x}{\log x}-3\int_{A/4}^{A/2}\frac{x\mathrm{d}x}{\log x}-2.0472\int_{A/5}^{A/4}\frac{x\mathrm{d}x}{\log x}\\
&-0.1016\int_q^{A/5}\frac{x\mathrm{d}x}{\log x},
\end{aligned}$$

所以将积分中的 $x$ 换成 $Ax$ 即得引理.

## 6. 较小二次非剩余的增长性

**引理 32** 命 $p\equiv 1 \pmod 4$, $p>10^6$ 及 $q_1=3$, 则 $5q_2q_3<p$.

**证明** 假定引理不成立, 即 $5q_2q_3\geqslant p$. 则

$$q_3 > (p/5)^{1/2}. \tag{1}$$

由 I，引理 7, 我们得 $q_3 \leqslant 4p^{1/2}/\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 7.5p^{1/2}$.

若 $q_2 < p^{1/2}/37.5$, 则引理立即成立. 若 $q_2 \geqslant p^{1/2}/37.5$, 则由引理 26 得

$$q_2 > p^{1/2}/15. \tag{2}$$

所以引理当 $q_2 \leqslant p^{1/2}/15$ 时成立, 因此我们可以假定

$$q_2 > p^{1/2}/15. \tag{3}$$

由 I, 引理 10 得

$$\begin{aligned}\frac{1}{2}\sum_{a=1}^{A}\sum_{n=1,3\nmid n}^{a}\left(1-\left(\frac{n}{p}\right)\right) &\leqslant \sum_{a=q_3}^{A}\left(\sum_{q_3\leqslant q\leqslant a}\left[\frac{a}{q}\right]-\sum_{q_3\leqslant q\leqslant a/3}\left[\frac{a}{3q}\right]\right)\\ &\quad+\sum_{a=q_2}^{A}\left(\left[\frac{a}{q_2}\right]-\left[\frac{a}{3q_2}\right]\right)\\ &=\sum_{a=q_2}^{A}\left(\sum_{\nu=1}^{[a/q_3]}\pi\left(\frac{a}{\nu}\right)-\left[\frac{a}{q_3}\right](\pi(q_3)-1)\right.\\ &\quad\left.-\sum_{\nu=1}^{[a/3q_3]}\pi\left(\frac{a}{3\nu}\right)+\left[\frac{a}{3q_3}\right](\pi(q_3)-1)\right)\\ &\quad+\sum_{a=q_2}^{A}\left(\left[\frac{a}{q_2}\right]-\left[\frac{a}{3q_2}\right]\right).\end{aligned}$$

将不等式的第一边记为 $S_0$. 则

$$\begin{aligned}S_0 &< \sum_{a=q_2}^{A}\sum_{\nu=1,3\nmid\nu}^{[a/q_3]}\pi\left(\frac{a}{\nu}\right)-\sum_{a=q_3}^{A}\left(\left[\frac{a}{q_3}\right]-\left[\frac{a}{3q_3}\right]\right)(\pi(q_3)-1)\\ &\quad+\sum_{a=q_2}^{A}\left(\left[\frac{a}{q_2}\right]-\left[\frac{a}{3q_2}\right]\right)=S'-S''+S''' \ (\text{定义}).\end{aligned} \tag{4}$$

(1) 假定 $p > 10^8$, 我们取 $A = [10p^{1/2}]$. 由于 $A^2/3 > (100p - 20p^{1/2})/3 = 33.32p + 4p/300 - 20p^{1/2}/3 > 33.32p$. 所以由引理 25 可知

$$\begin{aligned}S_0 &> (A^2/3 - 41Ap^{1/2}/81 - 0.21256p)/2\\ &> (33.32 - 5.1 - 0.22)p/2 = 14p.\end{aligned} \tag{5}$$

由 (3) 得

$$
\begin{aligned}
S''' &< \sum_{a=q_2}^{A}\left(\frac{a}{q_2}-\frac{a}{3q_2}+1\right) < \frac{A(A+1)}{3q_2}+A\\
&< 50(10p^{1/2}+1)+10p^{1/2}=510p^{1/2}+50\\
&< 0.06p. \qquad (6)
\end{aligned}
$$

由于 $q_3 > (p/5)^{1/2} \geqslant 10^4/5^{1/2} > 51^2$, 所以由 I , 引理 2 可知

$$
S'' > (0.9607\mathrm{li}q_3 - 2.7)\sum_{a=q_3}^{A}\left(\left[\frac{a}{q_3}\right]-\left[\frac{a}{3q_3}\right]\right).
$$

由引理 27 及 (2) 得

$$
\begin{aligned}
\sum_{a=q_3}^{A}\left(\left[\frac{a}{q_3}\right]-\left[\frac{a}{3q_3}\right]\right) &> \frac{1}{2q_3}((A+2)(A-q_3)\\
&\quad -\frac{1}{3}\left(A+1-\frac{3q_3}{2}\right)^2\Big)\\
&= \frac{1}{2q_3}\left(\frac{2}{3}A^2+\frac{4}{3}A-\frac{3}{4}q_3^2-q_3-\frac{1}{3}\right)\\
&> \frac{p}{q_3}\left(\frac{100}{3}-\frac{1}{3\times 10^8}-\frac{3^3}{8}-\frac{3}{2\times 10^4}-\frac{1}{6\times 10^8}\right)\\
&> \frac{29.957}{q_3}p.
\end{aligned}
$$

所以

$$
\begin{aligned}
S'' &> (29.957/q_3)(0.9607\mathrm{li}q_3-2.7)\\
&> (28.779\mathrm{li}q_3/q_3-0.03)p. \qquad (7)
\end{aligned}
$$

最后由 I , 引理 2 及引理 31 可知

$$
\begin{aligned}
S' &< 1.0376\sum_{a=q_3}^{A}\sum_{\nu=1,3\nmid\nu}^{a/q_3}(\mathrm{li}a/\nu+1.85)\\
&< 1.0376\Big\{\frac{1}{6}A(A+2)\log\left(\log\frac{A}{4}\log\frac{A}{5}\right)\\
&\quad -\frac{1}{6}(2A^2+2A+9q_3)\log\log q_3+\frac{\mathrm{li}q_3}{12q_3}(4A^2+8A+q_3^2+4)\\
&\quad +\frac{0.03A}{\log A/5}+\frac{q_3^2}{8\log q_3}\left(\log\frac{A^2}{20q_3^2}+\frac{9}{20q_3}\right)\\
&\quad +A^2\Big(\int_{1/2}^{1}\frac{(1-x)\mathrm{d}x}{\log Ax}+\int_{1/4}^{1/2}\frac{(2-3x)\mathrm{d}x}{\log Ax}+\int_{1/5}^{1/4}\frac{(1.1667-2.0472)\mathrm{d}x}{\log Ax}
\end{aligned}
$$

$$+0.1016\int_{q_3/A}^{1/5}\frac{x\mathrm{d}x}{\log Ax}\biggr)+\mathrm{li}A+\mathrm{li}\frac{A}{2}\biggr\}$$
$$+1.91956\sum_{a=q_3}^{A}\left(\left[\frac{a}{q_3}\right]-\left[\frac{a}{3q_3}\right]\right).$$

由于

$$\frac{1}{6}A(A+2)\log\left(\log\frac{A}{4}\log\frac{A}{5}\right)-\frac{1}{6}(2A^2+2A+9q_3)\log\log q_3$$
$$<\frac{1.0001}{6}A^2\left(\log\frac{\log(5/2)p^{1/2}\log 2p^{1/2}}{(\log p^{1/2}-(\log 5)/2)^2}+\frac{2\log\log(p/5)^{1/2}}{[10p^{1/2}]}\right)$$
$$<\frac{1.0001}{6}A^2\left(\log\frac{(4\log 10+\log 2.5)(4\log 10+\log 2)}{(4\log 10-(\log 5)/2)^2}+0.0002\right)$$
$$<\frac{1.0001}{6}A^2\left(\log\frac{10.267\times 9.9035}{8.40562^2}+0.0002\right)$$
$$=\frac{1.001}{6}A^2(\log 1.42+0.0002)$$
$$<\frac{0.351}{6}A^2<5.85p,$$

$$\frac{\mathrm{li}q_3}{12q_3}(4A^2+8A+q_3^2+4)<\frac{\log q_3}{q_3}p\left(\frac{100}{3}+\frac{2\times 10}{3\times 10^4}+\frac{3^2}{12}+\frac{1}{3\times 10^8}\right)$$
$$<34.0841\mathrm{li}q_3p/q_3,$$

$$\frac{0.03A}{\log A/5}<\frac{0.3p^{1/2}}{\log(2p^{1/2}-1)}=\frac{0.3p}{10^4\log(2\times 10^4-1)}<0.00001p,$$

$$\frac{q_3^2}{8\log q_3}\left(\log\frac{A^2}{20q_3^2}+\frac{9}{20q_3}\right)<\frac{9p}{8\log(3p^{1/2})}\left(\log\frac{10^2\times 5}{20}+\frac{9(5)^{1/2}}{20\times 10^4}\right)$$
$$<\frac{9}{8\times 10.30895}(3.21889+0.0002)p<0.36p$$

(这里用到 $(p/5)^{1/2}<q_3<3p^{1/2}$).

$$\int_{1/2}^{1}\frac{(1-x)\mathrm{d}x}{\log Ax}<\frac{1}{\log A/2}\int_{1/2}^{1}(1-x)\mathrm{d}x=\frac{1}{8\times 10.81977}<0.0116,$$

$$\int_{1/4}^{1/2}\frac{(2-3x)\mathrm{d}x}{\log Ax}<\frac{7}{32\log A/4}<\frac{7}{32\times 10.126635}<0.0217,$$

$$\int_{1/5}^{1/4}\frac{(1.1667-2.0472x)\mathrm{d}x}{\log Ax}<\frac{1}{\log A/5}\left(\frac{1.1667}{20}-\frac{9\times 2.0472}{800}\right)<0.00357,$$

$$0.1016\int_{q_3/A}^{1/5}\frac{x\mathrm{d}x}{\log Ax}<\frac{0.00204}{\log q_3}<0.0001,$$

① 当 $\mathrm{e}^4\leqslant x$ 时, $\mathrm{li}x<x/(\log x-2)$. 事实上, 当 $x=\mathrm{e}^4$ 时, 不等式成立, 及 $\mathrm{dli}x/\mathrm{d}x\leqslant \mathrm{d}(x/(\log x-2))/\mathrm{d}x$.

$$\text{li}A + \text{li}A/2 < 2\text{li}A < 2 \times \frac{10p^{1/2}}{\log 10p^{1/2} - 2}①$$

$$< \frac{2p}{10^3(\log 10^5 - 2)} < 0.0003p$$

与

$$\sum_{a=q_3}^{A} \left( \left[ \frac{a}{q_3} \right] - \left[ \frac{a}{3q_3} \right] \right) \leqslant \frac{A(A+1)}{3q_3} + A < 0.0085p,$$

所以

$$\begin{aligned} S' &< 1.0376p\{5.85 + 34.0841\text{li}q_3/q_3 + 0.00001p + 0.36 \\ &\quad + 10^2(0.0116 + 0.0217 + 0.0036 + 0.0001) + 0.0003\} \\ &\quad + 1.91956 \times 0.0085p \\ &< p(1.0376 \times 10 + 0.02 + 1.0376 \times 34.084)\text{li}q_3/q_3) \\ &< p(10.40 + 35.366\text{li}q_3/q_3). \end{aligned} \tag{8}$$

由 (4), (5), (6), (7) 及 (8), 我们有 $14p < p(10.40+35.366\text{li}q_3/q_3)-(28.799\text{li}q_3/q_3-0.03)p + 0.06p$, 即

$$\begin{aligned} 14 &< 10.40 + 0.03 + 0.06 + 6.59\text{li}q_3/q_3 \\ &< 10.49 + 6.59 \times 1/(\log(10^4/5^{1/2}) - 2) < 12, \end{aligned}$$

这是荒唐的.

(2) 假定 $10^6 < p < 10^8$, 则我们取 $A = [6p^{1/2}]$. 由引理 25 得

$$\begin{aligned} S_0 &> (A^2/3 - 41Ap^{1/2}/81 - 0.21256p)/2 \\ &> (12 - 0.004 - 3.0371 - 0.21256)p/2 > 4.3731p. \end{aligned} \tag{5$'$}$$

由引理 27 可知, 当 $q_2 > p/5q_3$ 时有

$$\begin{aligned} S'' &< \frac{1}{2q_2}\left(\left(A - \frac{q_2}{2} + 1\right)^2 - \frac{(A+2)(A-3q_2)}{3}\right) \\ &= \frac{1}{2q_2}\left(\frac{2}{3}A^2 + \frac{4}{3}A + \frac{(q_2+2)^2}{4}\right) \\ &= \frac{1}{q_2}\left(\frac{1}{3}A^2 + \frac{2}{3}A + \frac{(q_2+2)^2}{8}\right) \\ &< \frac{p}{q_2}\left(12 + \frac{4}{10^3} + \frac{(q_2+2)^2}{8p}\right) \\ &< 5q_3\left(12.004 + \frac{(p+10q_3)^2}{200pq_3^2}\right), \end{aligned}$$

在此需注意由 (2) 可知, 函数在 $q_2 < q_3 < 3q^{1/2}$ 中是递减的. 由于

$$\frac{(p+10q_3)^2}{200pq_3^2}=\frac{1}{200p}\left(\frac{p}{q_3}+10\right)^2<\frac{1}{200}\left(5^{1/2}+\frac{10}{p^{1/2}}\right)^2$$
$$<\frac{1}{200}\left(5^{1/2}+\frac{1}{100}\right)^2<0.0253,$$

所以

$$S'''<60.1465q_3. \tag{6'}$$

由 $11<(p/5)^{1/2}<q_3<3p^{1/2}<10^6$, 所以由引理 18 可知 $S''>(\mathrm{li}q_3-\mathrm{li}q_3^{1/2}-1)\sum_{a=q_3}^{A}([a/q_3]-[a/3q_3])$.

由引理 27 及 (2), 如同 (1), 我们有

$$\sum_{a=q_3}^{A}\left(\left[\frac{a}{q_3}\right]-\left[\frac{a}{3q_3}\right]\right)>\frac{1}{2q_3}\left(\frac{2}{3}A^2+\frac{4}{3}A-\frac{3}{4}q_3^2-q_3-\frac{1}{3}\right)$$
$$>\frac{p}{2q_3}\left(\frac{2}{3}6^2-\frac{8}{p^{1/2}}+\frac{4}{3}\frac{6}{p^{1/2}}-\frac{3}{4}\frac{q_3^2}{p}-\frac{q_3}{p^{1/2}}-\frac{1}{p}\right)$$
$$>\frac{p}{2q_3}\left(24-\frac{3}{4}\frac{q_3^2}{p}-\frac{3}{p^{1/2}}-\frac{1}{p}\right)$$
$$>\frac{p}{2q_3}\left(23.9969-\frac{3}{4}\frac{q_3^2}{p}\right)>\frac{p}{q_3}\left(11.9984-\frac{3}{8}\frac{q_3^2}{p}\right),$$

$$\frac{1}{q_3}<\left(\frac{5}{p}\right)^{1/2}<\frac{p^{1/2}}{10^3}=0.002237,$$

$$\frac{\mathrm{li}q_3^{1/2}}{q_3}<\frac{\mathrm{li}(10^3/5^{1/2})^{1/2}}{10^3/5^{1/2}}<\frac{\mathrm{li}21.176}{447.21}<\frac{10.75}{447.21}<0.02405.$$

所以

$$S''>p(\mathrm{li}q_3/q_3-0.0263)(11.9984-3q_3^2/8p). \tag{7'}$$

最后, 由引理 17 及引理 31 得

$$S'=\sum_{a=q_3}^{A}\sum_{\nu=1,3\nmid\nu}^{q/q_3}\pi\left(\frac{a}{\nu}\right)<\sum_{a=q_3}^{A}\sum_{\nu=1,3\nmid\nu}^{q/q_3}\mathrm{li}\frac{a}{\nu}$$
$$<\frac{1}{6}A(A+2)\log\left(\log\frac{A}{4}\log\frac{A}{5}\right)-\frac{1}{6}(2A^2+2A+9q_3)\log\log q_3$$
$$+\frac{\mathrm{li}q_3}{12q_3}(4A^2+8A+q_3^2+4)+\frac{0.03A}{\log A/5}+\frac{q_3^2}{8\log q_3}\left(\log\frac{A^2}{20q_3^2}+\frac{9}{20q_3}\right)$$
$$+A^2\left(\int_{1/2}^{1}\frac{(1-x)\mathrm{d}x}{\log Ax}+\int_{1/4}^{1/2}\frac{(2-3x)\mathrm{d}x}{x\log Ax}\right.$$

$$+\int_{1/5}^{1/4}\frac{(1.1667-2.0472x)\mathrm{d}x}{\log Ax}+0.1016\int_{q_3/A}^{1/5}\frac{x\mathrm{d}x}{\log Ax}\Bigg)+\mathrm{li}A+\mathrm{li}\frac{A}{2}$$

$$<\frac{A^2}{3}\left\{\frac{1}{2}\left(1+\frac{2}{A}\right)\log\left(\log\frac{A}{4}\log\frac{A}{5}\right)-\log\log q_3+\frac{6\mathrm{li}A}{A^2}\right.$$

$$+\frac{\mathrm{li}q_3}{q_3}\left(1+\frac{2}{A}+\frac{q_3^2}{4A^2}+\frac{1}{A^2}\right)+\frac{0.09}{A\log A/5}$$

$$+\frac{3q_3^2}{8A^2\log q_3}\left(\log\frac{A^2}{20q_3^2}+\frac{9}{20q_3}\right)+3\Bigg(\int_{1/2}^{1}\frac{(1-x)\mathrm{d}x}{\log Ax}$$

$$+\int_{1/4}^{1/2}\frac{(2-3x)\mathrm{d}x}{\log Ax}+\int_{1/5}^{1/4}\frac{(1.1667-2.0472x)\mathrm{d}x}{\log Ax}$$

$$\left.+0.1016\int_{q_3/A}^{1/5}\frac{x\mathrm{d}x}{\log Ax}\Bigg)\right\}.$$

由于

$$\frac{1}{A}\log\left(\log\frac{A}{4}\log\frac{A}{5}\right)<\frac{1}{5999}\log(\log 1500\log 1200)$$

$$<\frac{1}{5999}\log(7.31323\times 7.09008)<0.0007,$$

$$\frac{6\mathrm{li}A}{A^2}<\frac{6}{5999(\log 5999-2)}<0.00016,$$

$$\frac{0.09}{A\log A/5}<\frac{0.09}{599}9<0.00002,$$

$$\frac{3p}{8A^2\log q_3}\left(\log\frac{A^2}{20q_3^2}+\frac{9}{20q_3}\right)$$

$$<\frac{3}{286\log 10^3/5^{1/2}}\left(\log\frac{36}{4}+\frac{9(5)^{1/2}}{20\times 10^3}\right)<0.0038,$$

$$\int_{1/2}^{1}\frac{(1-x)\mathrm{d}x}{\log Ax}<\frac{1}{\log A/2}\int_{1/2}^{1}(1-x)\mathrm{d}x<\frac{1}{8.006}\times\frac{1}{8}<0.0157,$$

$$\int_{1/4}^{1/2}\frac{(2-3x)\mathrm{d}x}{\log Ax}<\frac{1}{\log A/4}\int_{1/4}^{1/2}(2-3x)\mathrm{d}x<0.03,$$

$$\int_{1/5}^{1/4}\frac{(1.1667-2.0472x)\mathrm{d}x}{\log Ax}$$

$$<\frac{1}{\log A/5}\int_{1/5}^{1/4}(1.1667-2.0472x)\mathrm{d}x<0.005,$$

$$0.1016\int_{q_3/A}^{1/5}\frac{x\mathrm{d}x}{\log Ax}<0.1016\times\frac{0.002}{\log q_3}<\frac{0.1016\times 0.002}{6.103}<0.0001,$$

及最后四个积分的总和小于 0.0508, 所以

$$
\begin{aligned}
S' < 12p\Big\{&\frac{1}{2}\log\left(\log\frac{A}{4}\log\frac{A}{5}\right) - \log\log q_3 \\
&+ \frac{\mathrm{li}q_3}{q_3}\left(1 + \frac{2}{5.999p^{1/2}} + \frac{q_3^2}{143.952p} + 0.00001\right) \\
&+ 0.0038\frac{q_3^2}{p} + 0.15328\Big\}
\end{aligned} \tag{8'}
$$

(这里用到 $0.0007 + 0.00016 + 0.00002 + 3 \times 0.0508 = 0.15328$).

由 (4), (5′), (6′), (7′) 与 (8′) 得

$$
\begin{aligned}
&4.3731 < 12\Big\{\frac{1}{2}\log\left(\log\frac{A}{4}\log\frac{A}{5}\right) - \log\log q_3 \\
&+ \frac{\mathrm{li}q_3}{q_3}\left(1 + \frac{2}{5.999p^{1/2}} + \frac{q_3^2}{143.952p} + 0.00001\right) \\
&+ 0.0038\frac{q_3^2}{p} + 0.15328\Big\} \\
&- (\mathrm{li}q_3/q_3 - 0.0263)(11.9984 - 3q_3^2/8p) + 60.1465q_3/p, \\
&\frac{4.3731}{12} < \frac{1}{2}\log\left(\log\frac{A}{4}\log\frac{A}{5}\right) - \log\log q_3 \\
&+ \frac{\mathrm{li}q_3}{q_3}(0.00014 + 0.00034 + 0.03825q_3^2/p + 0.00001) \\
&+ 0.0263\left(1 - \frac{q_3^2}{32p}\right) + 0.0038q_3^2/p + \frac{60.1465}{12}\frac{q_3}{p} + 0.15328.
\end{aligned}
$$

由于

$$
\frac{\mathrm{li}q_3}{q_3} < \frac{1}{\log q_3 - 2} < \frac{1}{4.103} < 0.24373,
$$

所以

$$
\begin{aligned}
0.3644 < &\frac{1}{2}\log\left(\log\frac{A}{4}\log\frac{A}{5}\right) - \log\log q_3 \\
&+ 0.24373(0.00049 + 0.03825q_3^2/p) \\
&+ 0.0263(1 - q_3^2/32p) + 0.0038q_3^2/p \\
&+ 5.013q_3/p + 0.15328,
\end{aligned}
$$

即

$$
\begin{aligned}
0.3644 < &\frac{1}{2}\log\left(\log\frac{A}{4}\log\frac{A}{5}\right) - \log\log q_3 + 0.0123q_3^2/p \\
&+ 5.013q_3/p + 0.1797.
\end{aligned}
$$

因此

$$\log\log q_3 < \frac{1}{2}\log\left(\log\frac{A}{4}\log\frac{A}{5}\right) + 0.0123q_3^2/p + 5.013q_3/p - 0.1847. \tag{9}$$

由于 $(p/5)^{1/2} < q_3 < 3p^{1/2}$, 所以

$$\log\log q_3 < \frac{1}{2}\log\left(\log\frac{A}{4}\log\frac{A}{5}\right) + 0.0123\times 9 + \frac{5.013\times 3}{10^3} - 0.1847 < \frac{1}{2}\log\left(\log\frac{A}{4}\right)^2,$$

即

$$q_3 < (3/2)p^{1/2}. \tag{10}$$

对于 $p < 10^8$, 由 (10) 可知

$$\begin{aligned}&\frac{\mathrm{d}}{\mathrm{d}q_3}\left(\log\log q_3 - \frac{0.0123}{p}q_3^2 - \frac{5.013q_3}{p}\right)\\ &= \frac{1}{q_3\log q_3} - \frac{0.0246q_3}{p} - \frac{5.013}{p}\\ &> \frac{2}{3p^{1/2}\log((3/2)\times 10^4)} - \frac{0.0246}{p^{1/2}}\frac{3}{2} - \frac{5.013}{p} > 0.\end{aligned}$$

因此由 (9) 得

$$\begin{aligned}\log\log\left(\frac{p}{5}\right)^{1/2} &< \frac{1}{2}\log\left(\log\frac{3}{2}p^{1/2}\log\frac{6}{5}p^{1/2}\right)\\ &\quad + \frac{0.0123}{p}\left(\left(\frac{p}{5}\right)^{1/2}\right)^2 + \frac{5.013}{p}\left(\frac{p}{5}\right)^{1/2} - 0.1847\\ &< \frac{1}{2}\log\left(\log\frac{3}{2}p^{1/2}\log\frac{6}{5}p^{1/2}\right)\\ &\quad + 0.00246 + \frac{5.013}{10^3(5)^{1/2}} - 0.1847\\ &< \frac{1}{2}\log\left(\log\frac{3}{2}p^{1/2}\log\frac{6}{5}p^{1/2}\right) - 0.1799\end{aligned}$$

或

$$\begin{aligned}0.35 < 0.1799\times 2 &< \log\frac{\log(3p^{1/2}/2)\log(6p^{1/2}/5)}{(\log(p/5)^{1/2})^2}\\ &< \log\frac{\log(3/2\times 10^3)\log(6/5\times 10^3)}{(\log 10^3/5^{1/2})^2}\\ &< \log 1.393 < 0.332,\end{aligned}$$

这是荒唐的. 引理证完.

## 7. 证明定理的 E. A. 部分

**定理 4** 对于一个素数 $p \equiv 17 \pmod{24}$, 除可能 $p = 17, 41, 89, 113$ 与 137 之外, 在 $R(p^{1/2})$ 中没有 E. A.

**证明** (1) 假定 $q_2 = 5$, 由于

$$40q_3 < 7.5 \times 40p^{1/2} = 300p^{1/2} < p,$$

若 $p > 300^2 = 90000$, 则当 $p > 90000$ 时, 定理成立. 当 $p < 90000$ 时, 直接验证条件

$$40q_3 < p$$

可知, 除 $p = 17, 113, 233$ 与 257 之外均成立. 但

$$233 = 2 \cdot 5 \cdot q_3 + 41.3 \quad (q_3 = 11),$$

$$257 = 5q_3 + 74.3 \quad (q_3 = 7),$$

所以由 I, 引理 15 可知除可能 $p = 17, 113$ 与 137 之外, 在 $R(p^{1/2})$ 中均没有 E.A.

(2) 假定 $q_2 \neq 5$. 当 $p > 10^6$ 时, 由引理 32 及 I, 引理 16 可知定理成立. 当 $p \leqslant 10^6$ 时, 由直接验证可知除 $p = 41, 89$ 与 271 之外, 条件

$$5q_2q_3 < p$$

成立. 但

$$271 = 3q_3 + q_2 \cdot 34 \quad (q_2 = 7, q_3 = 11).$$

所以由 I, 引理 14 即得定理.

(王元 译)

# 关于 Blichfeldt 定理的一个注记[①]

华罗庚 (国立清华大学)

命 $\sigma \geqslant 1$ 及 $\xi_1, \cdots, \xi_n$ 为 $n \geqslant 3$ 个实变量 $x_1, \cdots, x_n$ 的线性型, 其系数行列式 $\Delta \neq 0$. 为了简单起见, 我们假定 $|\Delta| = 1$. 命 $2s$ 个型, 有共轭复数对系数, 及其余的 $n-2s$ 个型有实系数. 则

$$|\xi_1|^\sigma + \cdots + |\xi_n|^\sigma \leqslant 1$$

定义了 $x$ 空间一个对称凸体, 其体积 $V(\sigma)$ 等于

$$2^n \frac{\{\Gamma(1+\alpha)\}^{n-2s}\{\pi\Gamma(1+2\alpha)/2^{1+2\alpha}\}^s}{\Gamma(1+n\alpha)} \quad (\alpha = 1/\sigma).$$

Minkowski 原则称: 若

$$r^n \geqslant 2^n V^{-1}(\sigma), \tag{1}$$

则有一个格子点 $(x_1, \cdots, x_n) \neq (0, \cdots, 0)$ 满足不等式

$$|\xi_1|^\sigma + \cdots + |\xi_n|^\sigma \leqslant r^\sigma.$$

当 $\sigma \geqslant 2$ 时, 用 Blichfeldt 方法, von der Corput 与 Schaake[②]改进了这一结果. 他们的方法的关键一步为一个下面类型的不等式

$$\sum_{p \cdot q=1}^{k} |Z_p - Z_q|^\sigma \leqslant \varepsilon(\sigma) k \cdot \sum_{p=1}^{k} |Z_p|^\sigma, \tag{2}$$

此处 $\varepsilon(\sigma)$ 既不依赖于任意复数 $Z_p$, 亦不依赖于 $k$, 一旦有了这样一个不等式, 则 (1) 可以换成

$$r^n \geqslant (\varepsilon(\sigma))^{n/\sigma} \cdot \frac{n+\sigma}{\sigma} \cdot V^{-1}(\sigma). \tag{3}$$

初等的关系式

$$|u-v|^\sigma \leqslant 2^{\sigma-1}(|u|^\sigma + |v|^\sigma)$$

① 1945 年 2 月 24 日收到. 发表于*Bull. Amer. Math. Soc.*, 1945, 51: 537–539.

② *Acta Arithmetica*, 1936, 2: 152–160.

(基于当 $x>0$ 时, $x^\sigma$ 为 $x$ 的凸函数这一事实) 推出 (2), 其中 $\varepsilon(\sigma)=2^\sigma$. 将它代入 (3), 则并无改进. 反而更坏于 Minkowski 不等式. 无论如何, 当 $\sigma\geqslant 2$ 时, van dev Corput 与 Schaake 得到了较好的值 $2^{\sigma-1}$. 在此, 我将证明, 当 $1\leqslant\sigma\leqslant 2$ 时, $\varepsilon(\sigma)=2$ 是一个合理的选取, 而且这两种情况几乎立即可以从 Riesg 凸性定理中推出来.

事实上, 取 $\gamma=\alpha$ 及 $\chi$ 为线性型 $\chi_{pq}=Z_p-Z_q$ 即得这一定理的特殊化 (Hardy, Littlewood and Polya. *Inequalilies,p.*219, Theorem 296). 从而对于固定的 $k$ 及变量 $Z_1,\cdots,Z_k$,

$$\left\{\sum_{p\cdot q=1}^{k}|Z_p-Z_q|^{1/\alpha}/k\sum_{p=1}^{k}|Z_p|^{1/\alpha}\right\}^\alpha$$

的极大值 $M_k(\alpha)$ 是 $\alpha$ 的一个凸函数, 其中 $0\leqslant\alpha\leqslant 1$. 我们易于验证

$$M_k(0)=2,\quad M_k(1/2)=2^{1/2},\quad M_k(1)=2(1-1/k)\leqslant 2.$$

关于

$$\left\{\sum_p|Z_p|^{1/\alpha}\right\}^\alpha\to\max|Z_p|,\quad \alpha\to 0,$$

由 $\max|Z_p-Z_q|\leqslant 2\max|Z_p|$ 及当 $Z_1=1,Z_2=-1,Z_3=\cdots=Z_k=0$ 时达到上界 2, 即可得第一个方程. 类似地由初等不等式

$$\sum_{p\cdot q}|Z_p-Z_q|^2=2k\sum_p|Z_p|^2-2\left|\sum_p Z_p\right|^2\leqslant 2k\sum_p|Z_p|^2,$$

$$\sum_{p\neq q}|Z_p-Z_q|\leqslant\sum_{p\neq q}(|Z_p|+|Z_q|)=2(k-1)\sum_p|Z_p|,$$

及对应的关于 $Z_p$ 的选取达到上界的明显观察, 即得其他两个方程.

我们用 2 作为对数的基底, 则当 $\alpha=0,1/2,1$ 时, $\log_2 M_2(\alpha)$ 分别等于 1, 1/2 及小于或等于 1 之数, 从而折线

$$\begin{cases}1-\alpha, & \text{当 } 0\leqslant\alpha\leqslant 1/2,\\ \alpha, & \text{当 } 1/2\leqslant\alpha\leqslant 1\end{cases}$$

给出了凸函数 $\log_2 M_k(\alpha)$ 的一个上界, 从而我们获得 (2) 的可允许结果, 其中

$$\varepsilon(\sigma)=2^{\sigma-1},\text{当 }\sigma\geqslant 2;\quad \varepsilon(\sigma)=2,\text{当 }1\leqslant\sigma\leqslant 2 \tag{4}$$

这两种选择都是臻于至善的, 当 $0\leqslant\alpha\leqslant 1/2$ 时, 这可以由例子 $k=2,Z_1=-Z_2=1$ 来阐明, 而当 $1/2\leqslant\alpha\leqslant 1$ 时, 则可以由例子 $Z_1=-Z_2=1,Z_3=\cdots=Z_k=0$ 来阐明, 其中 $k$ 充分大.

考虑情况 $1 \leqslant \sigma \leqslant 2$, 若我们将 $\varepsilon(\sigma) = 2$ 代入 (3), 则我们将发现它不能改进 Blichfeldt 已有的不等式, 特别不能对最有兴趣的情况 $\sigma = 1$ 有所改进, 我们注意到

$$\left(\frac{|\xi_1|^\sigma + \cdots + |\xi_n|^\sigma}{n}\right)^{1/\sigma}$$

是指数 $\sigma$ 的一个递增函数, 而由 (3) 导出的格子极小

$$\left(\frac{2}{n}\right)^{1/\sigma} \left(\frac{n+\sigma}{\sigma}\right)^{1/n} (V(\sigma))^{-1/n}, \tag{5}$$

则不是递增的. 结于 $s = 0$, 当 $n \to \infty$ 时, (5) 趋于一个极限, 即

$$\frac{1}{2}\left(\frac{2}{\sigma \mathrm{e}}\right)^{1/\sigma} \Big/ \Gamma\left(1 + \frac{1}{\sigma}\right) = 2^{\alpha-1}\left(\frac{\alpha}{\mathrm{e}}\right)^{\alpha} \Big/ \Gamma(1+\alpha).$$

这一函数关于 $\alpha$ 的对数微商当 $\alpha = 1/2$ 时为负的, 而当 $\alpha = 2/3$ 时为正的, 从而这一函数在 $\sigma = 2$ 与 $\sigma = 1.5$ 之间有一个极小值; 数值计算给出其位置为 $\sigma = \sigma_0 = 1.8653\cdots$①. 在这一点的函数值

$$\leqslant 1/(3.146\mathrm{e})^{1/2},$$

它比 Blichfeldt 的常数②

$$1/(\pi \mathrm{e})^{\frac{1}{2}}$$

略好一点.

总之, 当 $2 \geqslant \sigma \geqslant \sigma_0$ 时, (1) 可以换成

$$r^n \geqslant 2^{n/\sigma}\left(\frac{n+\sigma}{\sigma}\right) V^{-1}(\sigma),$$

而当 $1 \leqslant \sigma \leqslant \sigma_0$ 时, 则 (1) 可以换成

$$r^n \geqslant 2^{n/\sigma_0}\left(\frac{n+\sigma_0}{\sigma_0}\right) V^{-1}(\sigma_0).$$

无论如何, $\sigma_0$ 的选取范围为 $1 \leqslant \sigma_0 \leqslant 2$ 时, 这将成立; 当 $n \to \infty$(及 $s = 0$), 我们的特殊选择趋于最佳. 即使对于小的 $n$, 这也已足够精确地去改进一点 Blichfeldt 的记录.

(王元　译)

① 作者感谢 Sge 先生给出这一数值.

② *Trans. Amer. Math. Soc.*, 1914, 15: 227–235.

# 关于 Wright 一个结果的改进①

华罗庚 (美国 Illinois 大学)

E. M. Wright 在他的文章 *The Prouhet-Lehmer Problem* [1] 中称: "我未发现 $W(k,s)$ 独立于 $s$ 的一个上界". 在此我将给出一个上界, 命 $W(k,s)$ 为最小的整数 $j$ 满足: 对于所有适合 $p \neq q$ 的 $p, q$, 存在整数 $x_{iu}(1 \leqslant i \leqslant j, 1 \leqslant u \leqslant s)$ 使

$$\sum_{i=1}^{j} x_{i1}^{h} = \sum_{i=1}^{j} x_{i2}^{h} = \cdots = \sum_{i=1}^{j} x_{is}^{h} \quad (1 \leqslant h \leqslant k), \tag{1}$$

$$\sum_{i=1}^{j} x_{ip}^{k+1} \neq \sum_{i=1}^{j} x_{iq}^{k+1}. \tag{2}$$

另一个由 Lehmer 定义的函数 $L(k,s)$[2], 其定义与 $W(k,s)$ 类似. 除需将述语 "对于所有适合 $p \neq q$ 之 $p$, $q$" 改为 "至少有一对 $p, q$". 显然 $L(k,2) = W(k,2)$ 及 $L(k,s) \leqslant W(k,s)$, 应用我的方法[3], Wright[1] 证明了我的上界

$$j_0 = (k+1)\left(\left[\frac{\log \frac{1}{2}(k+2)}{\log(1+1/k)}\right] + 1\right), \tag{3}$$

对于 $L(k,2)$ 成立, 而对一般的 $L(k,s)$ 亦有效, 及

$$W(k,s) \leqslant (k+1)\left(\left[\frac{\log \frac{1}{2}(k(s-1)+2)}{\log(1+1/k)}\right] + 1\right).$$

在这篇文章里, 我将证明我的上界 (3) 对于 $W(k,s)$ 及任意 $s$ 皆成立, 即给出了一个独立于 $s$ 的上界, 这一结果显然是下面定理的推论:

**定理** 命 $j \geqslant j_0$, 则对于任意 $s$, 皆存在整数

$$N_1, \cdots, N_k; \quad M_1, \cdots, M_s \quad (M_{t_1} \neq M_{t_2}, \text{ 当 } t_1 \neq t_2),$$

① 1948 年 8 月 10 日收到. 发表于 *J. London Math. Soc.*, 1949, 24: 157-159.

使 $s$ 个丢番图方程组

$$R_t(1 \leqslant t \leqslant s): \quad \begin{cases} \sum_{i=1}^{j} x_{it}^h = N_h & (1 \leqslant h \leqslant k), \\ \sum_{i=1}^{j} x_{it}^{k+1} = M_t & (x_{it} \geqslant 0) \end{cases}$$

是可解的.

命 $\alpha_1, \cdots, \alpha_{k+1}$ 为文献 [3] 引理 1 中的整数集合, 其中用 $k+1$ 代替 $k$, 今后我们假定

$$\alpha_u P^{\beta^{v-1}} \leqslant y_{uv} \leqslant 2\alpha_u P^{\beta^{v-1}} \quad (1 \leqslant u \leqslant k+1, 1 \leqslant v \leqslant l),$$

此处 $\beta = k/(k+1)$ 命 $r(n_1, \cdots, n_k)$ 为

$$\sum_{u=1}^{k+1} \sum_{v=1}^{l} y_{uv}^h = n_h \quad (1 \leqslant h \leqslant k)$$

的解数.

存在一个整数集合 $N_1, \cdots, N_k$ 适合

$$r(N_1, \cdots, N_k) \geqslant c_1 P^{(k+1)^2(1-\beta^l) - \frac{1}{2}k(k+1)}, \tag{4}$$

此处 $c_1$(及以后的 $c_2, \cdots$) 为仅依赖于 $k$ 的正常数, 事实上, 不同 $y$ 集合的个数不少于

$$\frac{1}{2} \prod_{u=1}^{k+1} \prod_{v=1}^{l} \alpha_u P^{\beta^{v-1}} \geqslant c_2 P^{(k+1)(1+\beta+\cdots+\beta^{l-1})} = c_2 P^{(k+1)^2(1-\beta^l)}.$$

由于 $|n_k| \leqslant c_3 P^k$, 所以不同的 $n$ 集合的个数

$$\leqslant c_4 P^{1+2+\cdots+k} = c_4 P^{\frac{1}{2}k(k+1)}.$$

所以存在一个 $n$— 集合, 例如 $N_1, \cdots, N_k$ 满足

$$r(N_1, \cdots, N_k) \geqslant \frac{c_2}{c_4} P^{(k+1)^2(1-\beta^l) - \frac{1}{2}k(k+1)}.$$

方程组

$$\sum_{u=1}^{k+1} \sum_{v=1}^{l} y_{uv}^h = N_h \quad (1 \leqslant h \leqslant k+1)$$

的解数 $\leqslant c_5 P^{\frac{1}{2}k(k+1)(l-\beta^l)}$. 这一结果是 Wright[1] 之引理 2.

现在考虑

$$\sum_{u=1}^{k+1}\sum_{v=1}^{l} y_{uv}^{h} = N_h \quad (1 \leqslant h \leqslant k)$$

的所有解. 对于每一解, 我们皆有一个整数 $M$ 使

$$\sum_{u=1}^{k+1}\sum_{v=1}^{l} y_{uv}^{k+1} = M.$$

若 $M$ 的集合仅含有 $e(\leqslant s-1)$ 个不同的元素 $M_1, \cdots, M_e$, 则 $e$ 个方程组

$$\prod\nolimits_i (1 \leqslant i \leqslant e): \quad \begin{cases} \sum_{u=1}^{k+1}\sum_{v=1}^{l} y_{uv}^{h} = N_h \quad (1 \leqslant h \leqslant k), \\ \sum_{u=1}^{k+1}\sum_{v=1}^{l} y_{uv}^{k+1} = M_i \end{cases}$$

解的总数 $\leqslant c_5 e P^{\frac{1}{2}k(k+1)(1-\beta^l)}$ 对于 $l > \left\{\log \frac{1}{2}(k+2)\right\} / \log(1+1/k)$, 当 $P$ 充分大时, 我们有

$$c_5 e P^{\frac{1}{2}k(k+1)(1-\beta^l)} < c_1 P^{(k+1)^2(1-\beta^l)-\frac{1}{2}k(k+1)} \leqslant r(N_1, \cdots, N_r) \tag{5}$$

此为矛盾.

证明给了我们更多的东西, 例如, 我们可以得一个 $s$ 与未知数 $x_{ij}$ 大小之间的关系.

我愿借此机会改正我的文章[3] 的脚注中的一个错误. 在脚注的最后一行中, 语句 "假定 $s \geqslant ck^3 \log k$" 遗漏了, 这一断言在华[5] 中被作为定理 16, $p$. 133 证明了. 此外, 在文献 [6] 中, 我还宣布了这方面一个更好的结果.

## 参 考 文 献


[1] E. M. Wright. *Journal London Math. Soc.*, 1948, 23: 279–285.

[2] D. H. Lehmer. *Scripta Math.*, 1947, 13: 37–41.

[3] 华罗庚. *Quarterly. J.*, 1938, 9: 315-320.

[4] 华罗庚. *Quarterly. J.*, 1940, 11: 161-176.

[5] 华罗庚. *Travaux de l'Institute Math. Stekloff*, 1947, 22.

[6] 华罗庚. *Proc. Nat. Acad. Sci., U. S. A.*


(王元 译)

# 关于一个二重指数和①

华罗庚　闵嗣鹤 (数学系)

## 摘　要

设 $\kappa$ 为含 $p^m$ 个元的有限域. 设 $f(x,y)$ 是 $\kappa$ 上的 $n$ 次多项式, 但它不等价于一个单变量的多项式. 用 $S[a]$ 表示 $\kappa$ 中元 $a$ 的迹. 那么有

$$\sum_{x,y\in\kappa} \mathrm{e}^{2\pi \mathrm{i} S[f(x,y)]/p} = O(p^{m(2-\frac{2}{n})}),$$

其中 $x$ 和 $y$ 过 $\kappa$ 中的所有元, 而 $O$ 常数仅依赖于 $n$. 特别地, 对于 $n=3$, 我们有更精确的结果:

$$\sum_{x,y\in\kappa} \mathrm{e}^{2\pi \mathrm{i} S[f(x,y)]/p} = O(p^{m(2-\frac{3}{4})}).$$

虽然简要地描述证明的过程相当困难, 但我们还是要指出, 其中大量地用到了关于有限域中微分方程的解的结果.

贯穿全文, 我们总考虑含 $p^m$ 个元的有限域 $\kappa$, 其中 $p$ 是一个素数, $m$ 是一个正整数.

本文的目的是要证明下面的定理:

设 $f(x,y)$ 是 $n(\geqslant 4)$ 次多项式, 它不能表作 $\kappa$ 上的一个 $n$ 次单变量多项式. 则有

$$\sum_{\xi,\eta} \mathrm{e}^{2\pi \mathrm{i} S[f(\xi,\eta)]/p} = O(p^{m(2-\frac{2}{n})}),$$

其中 $\xi,\eta$ 独立地过域 $\kappa$ 中的所有元, 而 $O$ 常数仅依赖于 $n$.

特别地, 取 $\kappa$ 为 $\bmod p$ 剩余类所构成的域时, 我们有

$$\sum_{\xi=1}^{p}\sum_{\eta=1}^{p} \mathrm{e}^{2\pi \mathrm{i} f(\xi,\eta)/p} = O(p^{2-\frac{2}{n}}).$$

**定义**　设

$$f_1(x_1,\cdots,x_n),\cdots,f_n(x_1,\cdots,x_n)$$

① 1940 年 10 月 5 日收到. 发表于 *The Science Reports of National Tsing Hua University*, Ser. A, 1947, 4(4-6): 484-518.

为 $\kappa$ 上的 $n$ 个多项式. 令

$$J=J(f_1,\cdots,f_n)=\frac{D(f_1,\cdots,f_n)}{D(x_1,\cdots,x_n)}$$

表示 $f_1,\cdots,f_n$ 的 Jacobi 行列式. 我们把方程组

$$f_i(x_1,\cdots,x_n)=0,\quad i=1,\cdots,n$$

的解当中, 满足 $J\neq 0$ 者称为非奇异解, 而满足 $J=0$ 者称为奇异解.

**引理 1** 方程组

$$f_i(x_1,\cdots,x_n)=0,\quad i=1,\cdots,n \tag{1}$$

的非奇异解的个数为 $O(1)$.

**证明** $n=1$ 时, 引理显然. 假设引理对于 $n-1$ 个变量和 $n-1$ 个方程成立, 我们来证明它对于 $n$ 个变量和 $n$ 个方程也成立.

如果 $f_1,\cdots,f_n$ 不包含 $x_n$, 则 $J(f_1,\cdots,f_n)$ 恒等于 0. 因而, (1) 式没有非奇异解, 引理成立. 如果其中恰有一个包含 $x_n$, 不妨设为 $f_n$, 及 $(x_1^{(0)},\cdots,x_n^{(0)})$ 为 (1) 式的一个非奇异解, 则当 $x_\nu=x_\nu^{(0)}$ 时, 我们有

$$J(f_1,\cdots,f_n)=\frac{\partial f_n}{\partial x_n}J(f_1,\cdots,f_{n-1})\neq 0.$$

我们可见, $(x_1^{(0)},\cdots,x_{n-1}^{(0)})$ 为 $f_1=0,\cdots,f_{n-1}=0$ 的一个非奇异解, 而 $f_n(x_1^{(0)},\cdots,x_{n-1}^{(0)},x)$ 不恒等于 0. 由归纳法假设, 可知引理成立.

设 $f_i$ 关于 $x_n$ 的次数为 $\lambda_i$. 当 $\lambda_1+\cdots+\lambda_n\leqslant 1$ 时, 引理成立, 这是因为 (1) 式中至多有一个方程包含 $x_n$. 现在假设引理对于 $\lambda_1+\cdots+\lambda_n\leqslant\gamma$ 成立, 我们来证明它对于 $\lambda_1+\cdots+\lambda_n=\gamma+1$ 也成立.

不失一般性, 我们设

$$f_1=f_{1,0}x_n^{\lambda_1}+\cdots+f_{1,\lambda_1},\quad f_2=f_{2,0}x_n^{\lambda_2}+\cdots+f_{2,\lambda_2},$$

这里 $\lambda_1\geqslant\lambda_2\geqslant 1$, 而 $f_{1,i},f_{2,i}$ 为 $x_1,\cdots,x_{n-1}$ 的多项式.

考虑方程组

$$f_1'=f_{2,0}f_1-f_{1,0}x_n^{\lambda_1-\lambda_2}f_2=0^{①},\quad f_i=0\quad(i=2,\cdots,n). \tag{2}$$

显然, (1) 式的每一个解均为 (2) 式的解. 我们将证明, (1) 式的每一个非奇异解 $(x_1^{(0)},\cdots,x_n^{(0)})$, 如果满足 $f_{2,0}\neq 0$ 的话, 则它就是 (2) 式的非奇异解.

① 这个等式也可能会是恒等式, 如果这样的话, (2) 式就没有非奇异解了.

通过对 $x_i(i=1,\cdots,n)$ 微分 (2) 式中的第一个等式, 我们可得

$$\begin{aligned}\frac{\partial f_1'}{\partial x_i} =& f_{2,0}\frac{\partial f_1}{\partial x_i}-f_{1,0}x_n^{\lambda_1-\lambda_2}\frac{\partial f_2}{\partial x_i}+\frac{\partial f_{2,0}}{\partial x_i}f_1-\frac{\partial f_{1,0}}{\partial x_i}x_n^{\lambda_1-\lambda_2}f_2\\ &\left(=f_{2,0}\frac{\partial f_1}{\partial x_i}-f_{1,0}x_n^{\lambda_1-\lambda_2}\frac{\partial f_2}{\partial x_i},\ \text{当 } x_\nu=x_\nu^{(0)} \text{ 时}\right),\quad i=1,\cdots,n-1, \qquad (3)\\ \frac{\partial f_1'}{\partial x_n} =& f_{2,0}\frac{\partial f_1}{\partial x_n}-f_{1,0}x_n^{\lambda_1-\lambda_2}\frac{\partial f_2}{\partial x_n}+\frac{\partial f_{2,0}}{\partial x_n}f_1-\frac{\partial f_{1,0}}{\partial x_n}x_n^{\lambda_1-\lambda_2}f_2\\ &-(\lambda_1-\lambda_2)f_{1,0}x_n^{\lambda_1-\lambda_2-1}f_2\\ &\left(=f_{2,0}\frac{\partial f_1}{\partial x_n}-f_{1,0}x_n^{\lambda_1-\lambda_2}\frac{\partial f_2}{\partial x_n},\ \text{当 } x_\nu=x_\nu^{(0)} \text{ 时}\right).\end{aligned}$$

因此

$$J(f_1',f_2,\cdots,f_n)=f_{2,0}J(f_1,f_2,\cdots,f_n)\neq 0,\quad \text{当 } x_\nu=x_\nu^{(0)} \text{ 时}.$$

现在假设 $(x_1^{(0)},\cdots,x_n^{(0)})$ 是 (1) 式的一个非奇异解, 它满足 $f_{2,0}=0$, 于是, 此解既满足

$$f_1=0,\quad f_2'=f_2-f_{2,0}x_n^{\lambda_2}=0,\quad f_i=0\quad (i=3,\cdots,n), \qquad (4)$$

又满足

$$f_1=0,\quad f_{2,0}=0,\quad f_i=0\quad (i=3,\cdots,n). \qquad (5)$$

由 (4) 式知

$$\frac{\partial f_2'}{\partial x_i}=\frac{\partial f_2}{\partial x_i}-\frac{\partial f_{2,0}}{\partial x_i}x_n^{\lambda_2},\quad i=1,\cdots,n-1, \qquad (6)$$

$$\frac{\partial f_2'}{\partial x_n}=\frac{\partial f_2}{\partial x_n}-\lambda_2 f_{2,0}x_n^{\lambda_2-1}\quad\left(=\frac{\partial f_2}{\partial x_n},\ \text{当 } x_\nu=x_\nu^{(0)} \text{ 时}\right).$$

因此

$$0\neq J(f_1,\cdots,f_n)=J(f_1,f_2',f_3,\cdots,f_n)+x_n^{\lambda_2}J(f_1,f_{2,0},f_3,\cdots,f_n),\quad \text{当 } x_\nu=x_\nu^{(0)} \text{ 时}.$$

由此可知, $J(f_1,f_2',f_3,\cdots,f_n)$ 与 $J(f_1,f_{2,0},f_3,\cdots,f_n)$ 不能同时为 0.

由上面的讨论知, (1) 式的每一个非奇异解必定是方程组 (2), (4) 与 (5) 之一的非奇异解. 因为每个方程组关于 $x_n$ 的次数之和都 $\leqslant\gamma$, 所以, 它们中的每一个的非奇异解的个数均为 $O(1)$. 因此, (1) 式仅有 $O(1)$ 个非奇异解.

**引理 2**　设 $f(x_1,\cdots,x_n)(\neq 0)$ 是 $\kappa$ 上的多项式, 则方程

$$f(x_1,\cdots,x_n)=0 \qquad (7)$$

的解数为 $O(p^{m(n-1)})$.

**证明** $n=1$ 时, 引理显然. 假设 $n=s-1$ 时, 引理成立. 设

$$f(x_1,\cdots,x_s)=g_0(x_1,\cdots,x_{s-1})x_s^k+\cdots+g_k(x_1,\cdots,x_{s-1}),$$

其中 $g_i$ 为多项式, $g_0\neq 0$. 显然, 方程

$$f(x_1,\cdots,x_s)=0,\quad g_0(x_1,\cdots,x_{s-1})\neq 0$$

的解数为 $O(p^{m(s-1)})$. 而由归纳法假设, 方程

$$f(x_1,\cdots,x_s)=0,\quad g_0(x_1,\cdots,x_{s-1})=0$$

的解数为 $O(p^{m(s-2)}p^m)=O(p^{m(s-1)})$. 合之可得, 方程

$$f(x_1,\cdots,x_s)=0$$

的解数为 $O(p^{m(s-1)})$, 由此可得引理.

**引理 3** 设 $g(u)$ 是一个 $s(<p)$ 次的多项式, 它满足

$$A(u)g'(u)+B(u)g(u)=0,\tag{8}$$

其中 $A(u),B(u)$ 是多项式. 则 $g(u)$ 的每一个不可约因子都是 $A(u)$ 的因子.

**证明** 令 $h(u)$ 为 $g(u)$ 的一个不可约因子, 并设

$$(h(u))^\nu\|g(u)^{①}.$$

于是, 因为 $\nu<p$, 所以

$$(h(u))^{\nu-1}\|g'(u).$$

由 (8) 式知

$$h(u)|A(u).$$

**引理 4** 设 $A(u),B(u),C(u)$ 和 $D(u)$ 是多项式, 且

$$(A(u),A'(u)B(u))=1.$$

设 $g(u)$ 是一个 $s(<p)$ 次的多项式, 它满足

$$A(u)B(u)g'(u)-\left(A(u)C(u)+\frac{h}{k}A'(u)B(u)\right)g(u)+(A(u))^\mu D(u)=0,\tag{9}$$

① $(h(u))^\nu\|g(u)$ 表示 $(h(u))^\nu|g(u)$, 而 $(h(u))^{\nu+1}\nmid g(u)$.

其中 $h, k$ 为整数, 而 $h < p, \mu < \dfrac{h}{k} + 1$. 则

$$(A(u))^{\mu}|g(u).$$

**证明**　假设

$$g(u) = (A(u))^{\mu'}h(u), \quad A(u) \nmid h(u), \quad 0 \leqslant \mu' \leqslant \mu - 1.$$

代到 (9) 式中并除掉因子 $(A(u))^{\mu'}$, 我们有

$$A(u)B(u)h'(u) - \left(A(u)C(u) + \frac{h - k\mu'}{k}A'(u)B(u)\right)h(u) + (A(u))^{\mu-\mu'}D(u) = 0.$$

因为 $0 < h - k\mu' < p$, 所以, 我们有

$$A(u)|h(u),$$

但这与我们的假设正好相反. 因此,

$$(A(u))^{\mu}|g(u).$$

**引理 5**　设 $\beta(\neq 0)$ 是一个常数, $\lambda$ 和 $s$ 是整数, 它们满足 $3 \leqslant \lambda < p, 4 \leqslant s < p$. 设

$$c_i = c_i(\alpha) = c_i^{(0)} + c_i^{(1)}\alpha + \cdots, \quad i = 0, 1, \cdots, 5$$

为 $\alpha$ 的多项式, 不全为 0. 假设 $g(u)$ 是一个 $s$ 次多项式, 它与 $\alpha$ 无关, 且对于所有的 $\alpha$ 满足

$$(c_0u^2 + c_1u + c_2)g'(u) + (c_3u + c_4)g(u) = c_5(\beta u - \alpha)^{\lambda}. \tag{10}$$

则 $g(u)$ 的每一个不可约因子都是 $c_0u^2 + c_1u + c_2$ 的因子.

**证明**　如果 $c_5 = 0$, 由引理 3 立得结论. 假设 $c_5 \neq 0$, 且令

$$c_5 = c_5^{(0)} + \cdots + c_5^{(k)}\alpha^k, \quad c_5^{(k)} \neq 0, \quad c_5^{(\lambda)} = 0 \quad (\lambda < 0).$$

在 (10) 式的两边, 比较 $\alpha^{\lambda+k-j}(j = 0, 1, 2, 3)$ 的系数, 我们有

$$\begin{aligned}
&(c_0^{(\lambda+k)}u^2 + c_1^{(\lambda+k)}u + c_2^{(\lambda+k)})g'(u)\\
&+ (c_3^{(\lambda+k)}u + c_4^{(\lambda+k)})g(u) = (-1)^{\lambda}c_5^{(k)},
\end{aligned} \tag{11}$$

$$\begin{aligned}
&(c_0^{(\lambda+k-1)}u^2 + c_1^{(\lambda+k-1)}u + c_2^{(\lambda+k-1)})g'(u) + (c_3^{(\lambda+k-1)}u + c_4^{(\lambda+k-1)})g(u)\\
=&(-1)^{\lambda-1}\lambda\beta c_5^{(k)}u + (-1)^{\lambda}c_5^{(k-1)},
\end{aligned} \tag{12}$$

$$(c_0^{(\lambda+k-2)}u^2 + c_1^{(\lambda+k-2)}u + c_2^{(\lambda+k-2)})g'(u) + (c_3^{(\lambda+k-2)}u + c_4^{(\lambda+k-2)})g(u)$$

$$=(-1)^{\lambda-2}\binom{\lambda}{2}\beta^2 c_5^{(k)}u^2+(-1)^{(\lambda-1)}\lambda\beta c_5^{(k-1)}u+(-1)^{\lambda}c_5^{(k-2)}, \tag{13}$$

$$\begin{aligned}&(c_0^{(\lambda+k-3)}u^2+c_1^{(\lambda+k-3)}u+c_2^{(\lambda+k-3)})g'(u)+(c_3^{(\lambda+k-3)}u+c_4^{(\lambda+k-3)})g(u)\\=&(-1)^{\lambda-3}\binom{\lambda}{3}\beta^3 c_5^{(k)}u^3+(-1)^{\lambda-2}\binom{\lambda}{2}\beta^2 c_5^{(k-1)}u^2\\&+(-1)^{\lambda-1}\lambda\beta c_5^{(k-2)}u+(-1)^{\lambda}c_5^{(k-3)}.\end{aligned} \tag{14}$$

显然, $c_0^{(\lambda+k)},c_1^{(\lambda+k)},c_2^{(\lambda+k)}$ 不全为 0, 设它们之中第一个不为 0 者是 $c_i^{(\lambda+k)}(0\leqslant i\leqslant 2)$. 将 (11) 式乘以

$$\left((-1)^{\lambda-i-1}\binom{\lambda}{i+1}c_5^{(k)}\beta^{i+1}u^{i+1}+(-1)^{\lambda-i}\binom{\lambda}{i}c_5^{(k-1)}\beta^i u^i+\cdots\right.$$
$$\left.+(-1)^{\lambda}c_5^{(k-i-1)}\right)/(-1)^i c_5^{(k)},$$

并从 $(12+i)$ 式中减去所得的等式, 我们有

$$P(u)g'(u)+Q(u)g(u)=0,$$

其中 $P(u)$ 是 3 次多项式, 它的 $u^3$ 的系数为 $(-1)^i\binom{\lambda}{i+1}\beta^{i+1}c_i^{(\lambda+k)}\neq 0$. 因为 $g(u)$ 的次数 $\geqslant 4$, 所以, $g(u)$ 和 $g'(u)$ 必有一个非常数的公因子. 又因为公因子与 $\alpha$ 无关, 所以, 我们一定有 $c_5=0$, 但这与我们的假设正好相反.

**引理 6** 设 $\beta(\neq 0)$ 为常数. 设 $\lambda,\mu,h,k$ 为整数, 满足

$$h<p,\quad 2\leqslant\mu<\frac{h}{k}+1,\quad \mu-1\leqslant\lambda<p.$$

设 $C=C(\alpha),K=K(\alpha)$ 为 $\alpha$ 的多项式, $Q(u)=Q(u,\alpha)$ 为 $u$ 和 $\alpha$ 的多项式. 假设 $g(u)$ 是一个 $s(<p)$ 次的多项式, 它对于所有的 $\alpha$ 满足

$$C\left(ug'(u)-\frac{h}{k}g(u)\right)+u^{\mu}Q(u)=(\beta u-\alpha)^{\lambda}K. \tag{15}$$

则 $K=0$, 且 $u^{\mu}|g(u)$.

**证明** 令

$$ug'(u)-\frac{h}{k}g(u)=u^{\mu}q(u)+C_1u^{\mu-1}+\cdots+C_{\mu},$$

这里 $q(u)$ 为 $u$ 的多项式, 而 $C_i$ 与 $u$ 和 $\alpha$ 无关. 由 (15) 式可得

$$\begin{aligned}&C(C_1u^{\mu-1}+\cdots+C_{\mu})\\=&(-1)^{\lambda}K\left((-1)^{\mu-1}\binom{\lambda}{\mu-1}\alpha^{\lambda-\mu+1}\beta^{\mu-1}u^{\mu-1}+\cdots+\alpha^{\lambda}\right).\end{aligned}$$

因而

$$CC_i=(-1)^{\lambda+\mu-i}K\binom{\lambda}{\mu-i}\beta^{\mu-i}\alpha^{\lambda-\mu+i},\quad i=1,\cdots,\mu.$$

如果 $K\neq 0$, 则 $C_i\neq 0, i=1,\cdots,\mu$. 因此

$$CK^{-1}=(-1)^{\lambda+\mu-i}C_i^{-1}\binom{\lambda}{\mu-i}\beta^{\mu-i}\alpha^{\lambda-\mu+i},\quad i=1,\cdots,\mu.$$

但是这些等式不能同时成立, 所以, $K=0$. 由引理 4 可知，$u^\mu|g(u)$.

**引理 7**　设 $\beta(\neq 0)$ 为常数. 设 $h,\lambda,\mu$ 为整数, 满足

$$h<p,\quad 3\leqslant\mu<h+1,\quad 2\leqslant\lambda<p.$$

设

$$Q(u)=Q(u,\alpha)=Q_0(u)+Q_1(u)\alpha+\cdots+Q_\nu(u)\alpha^\nu,$$

其中 $Q_i(u)(i=0,\cdots,\nu)$ 为 $u$ 的多项式. 设

$$c_i=c_i(\alpha)=c_i^{(0)}+c_i^{(1)}\alpha+\cdots,\quad i=0,1,2$$

为 $\alpha$ 的多项式, 且 $c_i\neq 0$. 假设 $g(u)$ 是一个 $s(<p)$ 次的多项式, 它独立于 $\alpha$. 对于所有的 $\alpha$, 有

$$(c_0u+c_1)(ug'(u)-hg(u))+u^\mu Q(u)=(\beta u-\alpha)^\lambda c_2. \tag{16}$$

则 $c_2=0$, 且 $u^\mu|g(u)$.

**证明**　如果 $c_2=0$, 由引理 4 可得结论. 假设 $c_2\neq 0$. 令

$$c_2=c_2^{(0)}+\cdots+c_2^{(l)}\alpha^l,\quad c_2^{(l)}\neq 0.$$

在 (16) 式的两端, 比较 $\alpha^{\lambda+l-j}(j=0,1,2)$ 的系数, 我们有

$$\begin{aligned}&(c_0^{(\lambda+l)}u+c_1^{(\lambda+l)})(ug'(u)-hg(u))+u^\mu Q_{\lambda+l}(u)=(-1)^\lambda c_2^{(l)},\\&(c_0^{(\lambda+l-1)}u+c_1^{(\lambda+l-1)})(ug'(u)-hg(u))+u^\mu Q_{\lambda+l-1}(u)\\=&(-1)^{\lambda-1}\lambda c_2^{(l)}\beta u+(-1)^\lambda c_2^{(l-1)},\\&(c_0^{(\lambda+l-2)}u+c_1^{(\lambda+l-2)})(ug'(u)-hg(u))+u^\mu Q_{\lambda+l-2}(u)\\=&(-1)^{\lambda-2}\binom{\lambda}{2}c_2^{(l)}\beta^2u^2+(-1)^{\lambda-1}\lambda c_2^{(l-1)}\beta u+(-1)^\lambda c_2^{(l-2)}.\end{aligned}$$

显然, $c_0^{(\lambda+l)}$ 和 $c_1^{(\lambda+l)}$ 不全为 0. 如果前者不为 0, 我们将第一个等式乘以

$$((-1)^{\lambda-1}\lambda c_2^{(l)}\beta u+(-1)^\lambda c_2^{(l-1)})/(-1)^\lambda c_2^{(l)},$$

并从第二个等式中减去所得的等式. 否则, 我们将第一个等式乘以

$$\left((-1)^{\lambda-2}\binom{\lambda}{2}c_2^{(l)}\beta^2u^2+(-1)^{\lambda-1}\lambda c_2^{(l-1)}\beta u+(-1)^{\lambda}c_2^{(l-2)}\right)/(-1)^{\lambda}c_2^{(l)},$$

并从第三个等式中减去所得的等式. 在两种情形里, 所得到的等式均有形式

$$P(u)(ug'(u)-hg(u))+u^{\mu}R(u)=0,$$

其中 $P(u)$ 的次数为 2. 因为 $\mu\geqslant 3$, 所以

$$u|g(u).$$

由 (16) 式知, $c_2=0$, 但这与我们的假设正好相反.

**引理 8** 设 $\beta$ 和 $\tau$ 为两个非零常数. 设 $\lambda,\mu,h$ 为 $<p$ 的正整数. 设 $C=C(\alpha),K=K(\alpha)$ 为 $\alpha$ 的多项式, $Q(u)=Q(u,\alpha)$ 为 $u$ 和 $\alpha$ 的多项式. 假设 $g(u)$ 是一个 $s(<p)$ 次的多项式, 它独立于 $\alpha$, 对于所有的 $\alpha$ 满足

$$C((u^2+\tau)g'(u)-hug(u))+(u^2+\tau)^{\mu}Q(u)=(\beta u-\alpha)^{\lambda}K. \tag{17}$$

则 $K=0$, 且当 $h\geqslant 2\mu$ 时, 有

$$(u^2+\tau)^{\mu}|g(u).$$

**证明** 令

$$-hug(u)=(u^2+\tau)q(u)+l_1u+l_2u, \tag{18}$$

其中 $q(u)$ 是 $u$ 的多项式, 而 $l_1,l_2$ 独立于 $\alpha$ 和 $u$. 因为

$$\begin{aligned}(\beta u-\alpha)^{\lambda}=&-u\left(\sum_{i=0}^{[\frac{\lambda-1}{2}]}\binom{\lambda}{2i+1}\beta^{2i+1}\alpha^{\lambda-2i-1}u^{2i}\right)+\sum_{i=0}^{[\frac{\lambda}{2}]}\binom{\lambda}{2i}\beta^{2i}\alpha^{\lambda-2i}u^{2i}\\=&-u\left(\sum_{i=0}^{[\frac{\lambda-1}{2}]}(-1)^i\binom{\lambda}{2i+1}\beta^{2i+1}\tau^i\alpha^{\lambda-2i-1}\right)\\&+\sum_{i=0}^{[\frac{\lambda}{2}]}\binom{\lambda}{2i}(-1)^i\beta^{2i}\tau^i\alpha^{\lambda-2i}+(u^2+\tau)q_1(u)^{①},\end{aligned}$$

这里 $q_1(u)$ 是 $u$ 的多项式, 所以, 由 (17) 和 (18) 式, 我们有

$$C(l_1u+l_2)=K\left\{-u\left(\sum_{i=0}^{[\frac{\lambda-1}{2}]}(-1)^i\binom{\lambda}{2i+1}\beta^{2i+1}\tau^i\alpha^{\lambda-2i-1}\right)\right.$$

① $\left[\frac{\lambda-1}{2}\right]$ 和 $\left[\frac{\lambda}{2}\right]$ 分别表示 $\frac{\lambda-1}{2}$ 和 $\frac{\lambda}{2}$ 的整数部分.

$$+\sum_{i=0}^{[\frac{\lambda}{2}]}\binom{\lambda}{2i}(-1)^i\beta^{2i}\tau^i\alpha^{\lambda-2i}\Bigg\}.$$

如果 $K\neq 0$, 则上式可推出

$$l_1{:}l_2=-\left(\sum_{i=0}^{[\frac{\lambda-1}{2}]}(-1)^i\binom{\lambda}{2i+1}\beta^{2i+1}\tau^i\alpha^{\lambda-2i-1}\right):$$

$$\sum_{i=0}^{[\frac{\lambda}{2}]}\binom{\lambda}{2i}(-1)^i\beta^{2i}\tau^i\alpha^{\lambda-2i},$$

但这是不可能的. 因此, $K=0$, 由引理 4 知, $(u^2+\tau)^\mu|g(u)$.

**引理 9** 设 $f(x,y)$ 是 $\kappa$ 上的 $n$ 次多项式, $4\leqslant n\leqslant\sqrt{p}$. 设

$$F=f(\alpha t+\alpha',\beta t+\beta')=\sum_{i=0}^{n}A_it^i.$$

设矩阵

$$\begin{pmatrix} A_{n,\alpha} & \cdots & A_{1,\alpha}\\ A_{n,\beta} & \cdots & A_{1,\beta}\\ A_{n,\alpha'} & \cdots & A_{1,\alpha'}\\ A_{n,\beta'} & \cdots & A_{1,\beta'}\end{pmatrix} \tag{19}$$

的秩 $\leqslant 3$. 则由 $\kappa$ 上的一个非奇异线性变换, 可将 $f(x,y)$ 变为 $g(\xi,\eta)$, 后者或者关于 $\eta$ 的次数 $\leqslant\dfrac{n}{2}$, 或者是 $\xi^2+\tau\eta^2$ 的多项式.

**证明** 因为矩阵 (19) 的秩 $\leqslant 3$, 所以, 我们可以找到 4 个不全为 0 的 $\alpha,\alpha',\beta,\beta'$ 的多项式 $A,A',B,B'$, 使得

$$AA_{r,\alpha}+A'A_{r,\alpha'}+BA_{r,\beta}+B'A_{r,\beta'}=0,\quad r=1,\cdots,n.$$

因而

$$AF_\alpha+BF_\beta+A'F_{\alpha'}+B'F_{\beta'}=K,$$

这里 $K$ 是 $\alpha,\alpha',\beta,\beta'$ 的多项式, 因为 $F_\alpha=tF_{\alpha'}$, $F_\beta=tF_{\beta'}$, 所以, 我们有

$$(At+A')F_{\alpha'}+(Bt+B')F_{\beta'}=K. \tag{20}$$

令

$$f(x,y)=\sum_{i=0}^{n}f_i(x,y),$$

其中 $f_i(i=0,\cdots,n)$ 为 $i$ 次齐次多项式. 令

$$K=K_0+K_1+\cdots,$$

$$A = A_0 + A_1 + \cdots + A_h, \quad A' = A'_0 + A'_1 + \cdots + A'_h,$$

$$B = B_0 + B_1 + \cdots + B_h, \quad B' = B'_0 + B'_1 + \cdots + B'_h,$$

这里 $K_i, A_i, A'_i, B_i, B'_i$ 是 $\alpha, \alpha', \beta, \beta'$ 的 $i$ 次齐次多项式, 而 $A_h, A'_h, B_h, B'_h$ 不全为 0.

在 (20) 式的两端, 分别比较 $\alpha, \alpha', \beta, \beta'$ 的次数为 $n+h-1, \cdots$ 的项, 我们可得

$$\begin{aligned}
&\sum_{i=0}^{r}[(A_{h-r+i}t + A'_{h-r+i})f_{n-i,\alpha'}(\alpha t+\alpha', \beta t+\beta') \\
&+ (B_{h-r+i}t + B'_{h-r+i})f_{n-i,\beta'}(\alpha t+\alpha', \beta t+\beta')] \\
=&K_{n+h-r-1}, \quad r = 0, \cdots, n-1,
\end{aligned} \tag{21}$$

这里我们对于 $j<0$ 定义 $A_j = B_j = A'_j = B'_j = 0$.

令 $\dfrac{\alpha t+\alpha'}{\beta t+\beta'} = u$, 则有

$$t = -\frac{\beta' u - \alpha'}{\beta u - \alpha}, \quad \beta t + \beta' = \frac{\alpha'\beta - \alpha\beta'}{\beta u - \alpha}.$$

因而

$$f_{n-i}(\alpha t+\alpha', \beta t+\beta') = (\beta t+\beta')^{n-i} f_{n-i}(u),$$

其中 $f_{n-i}(u) = f_{n-i}(u, 1)$. 从而有

$$\begin{aligned}
f_{n-i,\alpha'}(\alpha t+\alpha', \beta t+\beta') &= (\beta t+\beta')^{n-i-1} f'_{n-i}(u) \\
&= \frac{(\alpha'\beta - \alpha\beta')^{n-i-1}}{(\beta u-\alpha)^{n-i-1}} f'_{n-i}(u), \\
f_{n-i,\beta'}(\alpha t+\alpha', \beta t+\beta') &= -(\alpha t+\alpha')(\beta t+\beta')^{n-i-2} f'_{n-i}(u) \\
&\quad + (n-i)(\beta t+\beta')^{n-i-1} f_{n-i}(u) \\
&= \frac{(\alpha'\beta - \alpha\beta')^{n-i-1}}{(\beta u-\alpha)^{n-i-1}}(-uf'_{n-i}(u) + (n-i)f_{n-i}(u)).
\end{aligned}$$

代到 (21) 式中并乘以 $(\beta u-\alpha)^n$, 我们可得

$$\begin{aligned}
&(\alpha'\beta - \alpha\beta')^{n-r-1}(\beta u-\alpha)^r\{[(A'_h - B'_h u)(\beta u - \alpha) \\
&- (A_h - B_h u)(\beta' u - \alpha')]f'_{n-r}(u) \\
&+ (n-r)[B'_h(\beta u-\alpha) - B_h(\beta' u - \alpha')]f_{n-r}(u)\} \\
&+ L_r(f_n(u), f'_n(u), \cdots, f_{n-r+1}(u), f'_{n-r+1}(u)) \\
&- (\beta u-\alpha)^n K_{n+h-r-1} = 0, \quad r = 0, \cdots, n-1,
\end{aligned} \tag{22}$$

这里 $L_r$ 为 $f_n(u),\cdots,f'_{n-r+1}(u)$ 的线性组合, 其系数是 $\alpha,\alpha',\beta,\beta'$ 和 $u$ 的多项式. (22) 式是关于 $\alpha,\alpha',\beta,\beta'$ 和 $u$ 的一个恒等式. 事实上, 对于满足 $\alpha'\beta-\alpha\beta'\neq 0$ 的任一组值 $\alpha,\alpha',\beta,\beta'$, (22) 式对于可能除 $-\dfrac{\alpha}{\beta}$ 外的所有的 $u$ 均满足. 因为 $mp>n+1$, 所以, (22) 式的左端乘以 $\alpha'\beta-\alpha\beta'$ 后恒等于 0. 因为 $\alpha'\beta-\alpha\beta'$ 不恒等于 0, 所以, (22) 式必为恒等式.

因为最大公因子 $(f_n(u),\cdots,f'_{n-r+1}(u))$ 与 $\alpha$ 和 $\beta$ 无关, 所以, 我们可以在 (22) 式的每一项中均除以 $(\beta u-\alpha)^r$, 从而得到

$$\begin{aligned}&(c_0u^2+c_1u+c_2)f'_{n-r}(u)-(n-r)(c_0u+c_3)f_{n-r}(u)\\&\quad+(f_n(u),\cdots,f'_{n-r+1}(u))Q_r(u)\\&=(\beta u-\alpha)^{n-r}K_{n+h-r-1},\end{aligned}\tag{23}$$

其中 $c_i$ 是 $\alpha,\alpha',\beta,\beta'$ 的多项式, 而 $Q_r(u)$ 是 $\alpha,\alpha',\beta,\beta'$ 和 $u$ 的多项式.

当 $r=0$ 时, 我们有

$$(c_0u^2+c_1u+c_2)f'_n(u)-n(c_0u+c_3)f_n(u)=(\beta u-\alpha)^nK_{n+h-1}.\tag{24}$$

不失一般性, 我们可设 $f_n(u)=f_n(u,1)$ 为 $n$ 次. 于是, 由引理 5 知, 存在三种情形:

1) $f_n(x,y)=\rho(\lambda_1x+\mu_1y)^k(\lambda_2x+\mu_2y)^{n-k},\ \dfrac{n}{2}<k<n$;

2) $f_n(x,y)=\rho(\lambda_1x+\mu_1y)^n$;

3) $f_n(x,y)=\rho(\lambda x^2+\mu xy+\nu y^2)^{\frac{n}{2}}$.①

不失一般性, 我们可设 $\rho=1,\lambda=1$. 在前两种情形里, 我们作变换 $\xi=\lambda_1x+\mu_1y,\eta=\lambda_2x+\mu_2y$, 而在最后一种情形里, 作变换 $\xi=x+\dfrac{\mu}{2},\eta=y$. 于是, 我们可将 $f_n(x,y)$ 分别简化为 $\xi^k\eta^{n-k},\xi^n$ 和 $(\xi^2+\nu\eta^2)^{\frac{n}{2}}$. 因此, 不失一般性, 我们可以假设 $f_n(x,y)$ 为以下三种情形之一:

1) $f_n(x,y)=x^ky^{n-k},\ \dfrac{n}{2}<k<n$;

2) $f_n(x,y)=x^n$;

3) $f_n(x,y)=(x^2+\tau y^2)^{\frac{n}{2}},\tau\neq 0$.

我们分别考虑这些情形.

**情形 1** $f_n(u)=u^k,\ \dfrac{n}{2}<k<n$.

由 (24) 式,

$$k(c_0u^2+c_1u+c_2)=n(c_0u+c_3)u.$$

---

① $\lambda x^2+\mu xy+\nu y^2$ 可以是不可约的, 也可以是可约的.

因而, $c_0=0$, 且

$$c_0u^2+c_1u+c_2=\frac{n}{k}c_3u.$$

代入 (23) 式中, 可得

$$\begin{aligned}&\frac{n}{k}c_3\left(uf'_{n-r}(u)-\frac{k(n-r)}{n}f_{n-r}(u)\right)+(f_n(u),\cdots,f'_{n-r+1}(u))Q_r(u)\\=&(\beta u-\alpha)^{n-r}K_{n+h-r-1}.\end{aligned}\tag{25}$$

当 $r=1$ 时, 我们有

$$u^{k-1}|(f_n(u),\cdots,f'_{n-r+1}(u)).$$

因为

$$k(n-1)<n^2<p,\quad 2\leqslant k-1<\frac{n-1}{n}k+1,\quad k-2<n-1<p,$$

所以, 由引理 6 可得, $K_{n+h-2}=0$ 且

$$u^{k-1}|f_{n-1}(u).$$

令 $f_n^*(u)=f_n(1,u),f_{n-1}^*(u)=f_{n-1}^*(1,u)$. 相似地, 我们可得

$$\begin{aligned}&\frac{n}{n-k}c_3^*\left(uf_{n-1}^{*'}(u)-(n-k)\frac{(n-1)}{n}f_{n-1}^*(u)\right)+(f_n^*(u),f_n^{*'}(u))Q_1^*(u)\\=&(\beta u-\alpha)^{n-1}K_{n+h-2}.\end{aligned}$$

因为 $K_{n+h-2}=0$ 和 $u^{n-k-1}|(f_n^*(u),f_n^{*'}(u))$, 所以, 由引理 4 可得

$$u^{n-k-1}|f_{n-1}^*(u).$$

因此

$$f_{n-1}(x,y)=x^{k-1}y^{n-k-1}(\rho x+\sigma y).$$

由变换 $x=\xi-\frac{\sigma}{k},y=\eta-\frac{\rho}{n-k}$, 我们可将 $f(x,y)$ 变成 $g(\xi,\eta)$, 后者不包含 $n-1$ 次项. 因而, 不失一般性, 我们可设 $f_{n-1}(u)=0$.

现在设

$$u^{k-s+1}|f_{n-s}(u),\quad s=1,\cdots,r-1,\quad r<\frac{n}{2}.$$

于是, 有

$$u^{k-r+1}|(f_n(u),\cdots,f'_{n-r+1}(u)).$$

因为

$$k(n-r)<n^2<p,\quad 2\leqslant k-r+1<\frac{n-r}{n}k+1,\quad k-r<n-r<p,$$

所以, 我们可将引理 6 用于 (25) 式, 得到

$$u^{k-r+1}|f_{n-r}(u)$$

或者

$$x^{k-r+1}|f_{n-r}(x,y).$$

因此, 当 $r<\frac{n}{2}$ 时, $f_{n-r}(x,y)$ 关于 $y$ 的次数 $<\frac{n}{2}$. 由此可得, $f(x,y)$ 关于 $y$ 的次数 $\leqslant\frac{n}{2}$.

**情形 2** $f_n(u)=u^n$.

由 (24) 式

$$c_0u^2+c_1u+c_2=(c_0u+c_3)u.$$

因而, (23) 式变成

$$\begin{aligned}&(c_0u+c_3)(uf'_{n-r}(u)-(n-r)f_{n-r}(u))+(f_n(u),\cdots,f'_{n-r+1}(u))Q_r(u)\\=&(\beta u-\alpha)^{n-r}K_{n+h-r-1}.\end{aligned}\tag{26}$$

首先, 假设 $c_3\neq 0$. 设

$$u^{n-s}|f_{n-s}(u),\quad s=0,\cdots,r-1,\quad r<\frac{n}{2}.$$

于是, 有

$$u^{n-r}|(f_n(u),\cdots,f'_{n-r+1}(u)).$$

因为

$$n-r<p,\quad 3\leqslant n-r<n-r+1,\quad 2<n-r<p,$$

所以, 我们用引理 7 可得

$$u^{n-r}|f_{n-r}(u)$$

或者

$$x^{n-r}|f_{n-r}(x,y),\quad r<\frac{n}{2}.$$

因此, $f(x,y)$ 关于 $y$ 的次数 $\leqslant\frac{n}{2}$.

其次, 假设 $c_3=0$. 设

$$u^{n-2s}|f_{n-s}(u),\quad s=0,\cdots,r-1.$$

于是, 有

$$u^{n-2r+1}|(f_n(u),\cdots,f'_{n-r+1}(u)).$$

当 $r\leqslant\frac{n}{2}$ 时, 由 (26) 式可得, $K_{n+h-r-1}=0$. 由引理 4 知

$$u^{n-2r}|f_{n-r}(u).$$

因此, $f_{n-r}(x,y)$ 关于 $y$ 的次数 $\leqslant\frac{n}{2}$.

**情形 3** $f_n(u)=(u^2+\tau)^{\frac{n}{2}}$.

由 (24) 式,

$$nu(c_0u^2+c_1u+c_2)=n(u^2+\tau)(c_0u+c_3).$$

因此, 我们可以找到一个依赖于 $\alpha,\alpha',\beta,\beta'$ 的常数 $c$, 使得

$$c_0u^2+c_1u+c_2=c(u^2+\tau),\quad c_0u+c_3=cu.$$

代入 (23) 式中, 我们有

$$\begin{aligned}&c((u^2+\tau)f'_{n-r}(u)-(n-r)f_{n-r}(u))+(f_n(u),\cdots,f'_{n-r+1}(u))Q_r(u)\\&=(\beta u-\alpha)^{n-r}K_{n+h-r-1}.\end{aligned}\tag{27}$$

当 $r=1$ 时, 我们有

$$(u^2+\tau)^{\frac{n}{2}-1}|(f_n(u),\cdots,f'_{n-r+1}(u)).$$

因为

$$n-1>1,n-1>2\left(\frac{n}{2}-1\right),$$

所以, 由引理 8 知

$$(u^2+\tau)^{\frac{n}{2}-1}|f_{n-1}(u).$$

因此

$$f_{n-1}(x,y)=(x^2+\tau y^2)^{\frac{n}{2}-1}(\rho x+\sigma y).$$

由变换 $x=\xi+\frac{\rho}{2},y=\eta+\frac{\sigma}{2}$, 我们可将 $f(x,y)$ 变成 $g(\xi,\eta)$, 后者不包含关于 $\xi,\eta$ 的 $n-1$ 次项. 因而, 不失一般性, 我们可设 $f_{n-1}(u)=0$.

当 $r=2$ 时, 因为

$$f_n(u)=(u^2+\tau)^{\frac{n}{2}},\quad f_{n-1}(u)=0,$$

所以, 有

$$(u^2+\tau)^{\frac{n}{2}-1}|(f_n(u),f'_n(u),\cdots,f_{n-1}(u),f'_{n-1}(u)).$$

又因为

$$n-2>1,\quad n-2=2\left(\frac{n}{2}-1\right),$$

所以, 由引得 8 知

$$(u^2+\tau)^{\frac{n}{2}-1}|f_{n-2}(u).$$

因此

$$f_{n-2}(x,y)=l(u^2+\tau)^{\frac{n}{2}-1}.$$

将 $f_n(x,y),f_{n-1}(x,y),f_{n-2}(x,y)$ 的表达式代到 (20) 式中, 比较两端关于 $t^n$, $t^{n-1},t^{n-2}$ 项的系数, 我们有

$$nA(\alpha^2+\tau\beta^2)^{\frac{n}{2}-1}\alpha+n\beta\tau(\alpha^2+\tau\beta^2)^{\frac{n}{2}-1}\beta=0, \tag{28}$$

$$\begin{aligned}&nA[\alpha'(\alpha^2+\tau\beta^2)^{\frac{n}{2}-2}((\alpha^2+\tau\beta^2)+(n-2)\alpha^2)\\&+\beta'(\alpha^2+\tau\beta^2)^{\frac{n}{2}-2}(n-2)\tau\alpha\beta]+nB[\cdots]\\&+nA'(\alpha^2+\tau\beta^2)^{\frac{n}{2}-1}\alpha+nB'\tau(\alpha^2+\tau\beta^2)^{\frac{n}{2}-1}\beta=0,\end{aligned} \tag{29}$$

$$\begin{aligned}&A\left[\frac{n}{2}\left\{\alpha'^2\frac{\partial^2}{\partial\alpha^2}(\alpha^2+\tau\beta^2)^{\frac{n}{2}-1}\alpha+2\alpha'\beta'\frac{\partial^2}{\partial\alpha\partial\beta}(\alpha^2+\tau\beta^2)^{\frac{n}{2}-1}\alpha\right.\right.\\&\left.\left.+\beta'^2\frac{\partial^2}{\partial\beta^2}(\alpha^2+\tau\beta^2)^{\frac{n}{2}-1}\alpha\right\}+(n-2)l(\alpha^2+\tau\beta^2)^{\frac{n}{2}-2}\alpha\right]\\&+B\left[\frac{n\tau}{2}\left\{\alpha'^2\frac{\partial^2}{\partial\alpha^2}(\alpha^2+\tau\beta^2)^{\frac{n}{2}-1}\beta+2\alpha'\beta'\frac{\partial^2}{\partial\alpha\partial\beta}(\alpha^2+\tau\beta^2)^{\frac{n}{2}-1}\beta\right.\right.\\&\left.\left.+\beta'^2\frac{\partial^2}{\partial\beta^2}(\alpha^2+\tau\beta^2)^{\frac{n}{2}-1}\beta\right\}+(n-2)l(\alpha^2+\tau\beta^2)^{\frac{n}{2}-2}\beta\right]\\&+nA'[\alpha'(\alpha^2+\tau\beta^2)^{\frac{n}{2}-2}(\alpha^2+\tau\beta^2+(n-2)\alpha^2)\\&+\beta'(\alpha^2+\tau\beta^2)^{\frac{n}{2}-2}(n-2)\tau\alpha\beta]+nB'[\cdots]=0.\end{aligned} \tag{30}$$

我们需要注意的仅仅是, 第一和第二个等式关于 $\alpha,\alpha',\beta,\beta'$ 是齐次的, (28) 式乘以 $\dfrac{n-2}{2}l(\alpha^2+\tau\beta^2)^{-1}$ 后, 再将它从 (30) 式中减去, 所得的等式关于 $\alpha,\alpha',\beta,\beta'$ 也是齐次的. 因此, 除去公因子 $D$ 之外, $A,A',B,B'$ 为关于 $\alpha,\alpha',\beta,\beta'$ 的 4 个齐次多项式. 因为由 (20) 式可得, 公因式 $D$ 一定整除 $K$, 所以, 不失一般性, 可以假设 $D=1$. 因此, 在 (21) 式中, 我们必须取

$$A_{h-r+i}=B_{h-r+i}=A'_{h-r+i}=B'_{h-r+i}=0,\quad i<r.$$

于是, 在 (23) 式中, 有 $Q_r(u)=0$. 从而, 我们有

$$c((u^2+\tau)f'_{n-r}(u)-(n-r)uf_{n-r}(u))=(\beta u-\alpha)^{n-r}K_{n+h-r-1}.$$

如果 $n-r \geqslant 1$, 由引理 8 知, $K_{n+h-r-1}=0$. 如果 $2|n-r$, 因为我们能取 $\mu=\dfrac{n-r}{2}$, 所以, 由引理 4 可得

$$(u^2+\tau)^{\frac{n-r}{2}} | f_{n-r}(u).$$

如果 $2 \nmid n-r$, 因为我们能取 $\mu=\left[\dfrac{n-r}{2}\right]+1<\dfrac{n-r}{2}+1$, 所以, 由引理 4, 我们可得

$$(u^2+\tau)^{[\frac{n-r}{2}]+1} | f_{n-r}(u).$$

在第二种情形里, $f_{n-r}(u)=0$. 因此, $f(x,y)$ 是 $x^2+\tau y^2$ 的多项式.

**引理 10** 设 $f(x)=a_0+a_1x+\cdots+a_nx^n (a_n \neq 0)$ 为 $\kappa$ 上的多项式. 则有

$$\sum_x \mathrm{e}^{2\pi \mathrm{i} S[f(x)]/p}=O(p^{m(1-\frac{1}{n})}), \tag{31}$$

这里 $x$ 过 $\kappa$ 中的所有元.

**证明** 令 $\theta$ 为 $\kappa$ 关于素域 $\varPi$ 的生成元. 于是, $\kappa$ 中的每个元 $x$ 可以记作

$$x=\alpha_0+\alpha_1\theta+\cdots+\alpha_{m-1}\theta^{m-1}, \quad \alpha_i \in \varPi.$$

因此

$$\begin{aligned}\sum_x \mathrm{e}^{2\pi \mathrm{i} S[ax]/p} &= \sum_{\alpha_0=1}^{p} \cdots \sum_{\alpha_{m-1}=1}^{p} \mathrm{e}^{2\pi \mathrm{i}(\alpha_0 S[a]+\cdots+\alpha_{m-1}S[a\theta^{m-1}])/p} \\ &= \begin{cases} p^m, & \text{如果对于所有的 } k, \text{ 有 } S[a\theta^k]=0, \\ 0, & \text{其他}. \end{cases}\end{aligned}$$

进一步地, 对于所有的 $k$ 有 $S[a\theta^k]=0$, 包含了 $a=0$. 事实上, 对于所有的 $x \in \kappa$, 我们有 $S[ax]=0$. 如果 $a \neq 0$, 则对于所有的 $x \in \kappa$, 有 $S[x]=0$, 但这是不可能的. 因此

$$\begin{aligned}&\sum_{b_1\in\kappa}\cdots\sum_{b_n\in\kappa}\left|\sum_{x\in\kappa}\mathrm{e}^{2\pi \mathrm{i} S[b_1x+\cdots+b_nx^n]/p}\right|^{2n} \\ =&\sum_{x_1\in\kappa}\cdots\sum_{x_n\in\kappa}\sum_{y_1\in\kappa}\cdots\sum_{y_n\in\kappa}{}^{\Delta} p^{mn}=n!p^{2mn},\end{aligned} \tag{32}$$

这里 $\Delta$ 表示求和条件

$$\begin{gathered} x_1+\cdots+x_n=y_1+\cdots+y_n, \\ \cdots\cdots \\ x_1^n+\cdots+x_n^n=y_1^n+\cdots+y_n^n. \end{gathered}$$

变换 $x=\lambda x'+\mu(\lambda \in \kappa, \mu \in \kappa, \lambda \neq 0)$ 可将 (31) 式变到 (32) 式中至少 $\dfrac{p^m(p^m-1)}{n}$ 个不同的项. 事实上, 如果

$$f(\lambda x+\mu)=f(x),$$

则

$$\lambda^n a_n = a_n,$$

$$n\lambda^{n-1}\mu\alpha_n + \lambda^{n-1}a_{n-1} = a_{n-1}.$$

第一个等式定出 $\lambda$, 它有至多 $n$ 个解. 第二个等式唯一地确定 $\mu$.

至此, 引理 10 得证.

**定理 1**　如果 $f(x,y)$ 是 $\kappa$ 上的 $n(\geqslant 4)$ 次多项式, $f(x,y)$ 不等于 $\kappa$ 上单变量的 $n$ 次多项式, 则有

$$\sum_x\sum_y \mathrm{e}^{2\pi \mathrm{i} S[f(x,y)]/p} = O(p^{m(2-\frac{2}{n})}),$$

这里 $x, y$ 独立地过 $\kappa$ 上的所有元.

**证明**　1) 假设 $f(\alpha t+\alpha', \beta t+\beta')$ 的任意 4 个系数的 Jacobi 行列式关于 $\alpha,\alpha',\beta,\beta'$ 恒等于 0. 由引理 9 知, 用 $\kappa$ 上的一个非奇异的线性变换, 可将 $f(x,y)$ 变为 $g(\xi,\eta)$, 后者或者是一个关于 $\eta$ 的次数 $\leqslant \dfrac{n}{2}$ 的多项式, 或者是一个 $\xi^2+\tau\eta^2$ 的多项式.

在第一种情形里, 令

$$g(\xi,\eta) = g_k(\xi)\eta^k + g_{k-1}(\xi)\eta^{k-1} + \cdots, g_k(\xi) \neq 0,\quad k \leqslant \frac{n}{2}.$$

由引理 10 可得

$$\begin{aligned}\left|\sum_x\sum_y \mathrm{e}^{2\pi \mathrm{i} S[f(x,y)]/p}\right| &= \left|\sum_\xi\sum_\eta \mathrm{e}^{2\pi \mathrm{i} S[g(\xi,\eta)]/p}\right| \\ &\leqslant \left|\sum_{\substack{\xi \\ g_k(\xi)\neq 0}}\sum_\eta \mathrm{e}^{2\pi \mathrm{i} S[g(\xi,\eta)]/p}\right| + \left|\sum_{\substack{\xi \\ g_k(\xi)=0}}\sum_\eta \mathrm{e}^{2\pi \mathrm{i} S[g(\xi,\eta)]/p}\right| \\ &\leqslant p^m \max_{g_k(\xi)\neq 0}\left|\sum_\eta \mathrm{e}^{2\pi \mathrm{i} S[g(\xi,\eta)]/p}\right| + O(p^m) \\ &= O(p^m p^{m(1-\frac{2}{n})}) + O(p^m) \\ &= O(p^{m(2-\frac{2}{n})}),\end{aligned}$$

除非 $g(\xi,\eta)$ 不包含 $\eta$.

在第二种情形里, 我们有

$$\left|\sum_x\sum_y \mathrm{e}^{2\pi \mathrm{i} S[f(x,y)]/p}\right| = \left|\sum_\xi\sum_\eta \mathrm{e}^{2\pi \mathrm{i} S[g(\xi^2+\tau\eta^2)]/p}\right|$$

$$\leqslant \left|\sum_{\xi}\sum_{\eta} \mathrm{e}^{2\pi \mathrm{i} S[g(\xi+\tau\eta)]/p}\right| + \left|\sum_{\xi}\sum_{\eta}\left(\frac{\xi}{\kappa}\right) \mathrm{e}^{2\pi \mathrm{i} S[g(\xi+\tau\eta)]/p}\right|$$
$$+ \left|\sum_{\xi}\sum_{\eta}\left(\frac{\eta}{\kappa}\right) \mathrm{e}^{2\pi \mathrm{i} S[g(\xi+\tau\eta)]/p}\right|$$
$$+ \left|\sum_{\xi}\sum_{\eta}\left(\frac{\xi}{\kappa}\right)\left(\frac{\eta}{\kappa}\right) \mathrm{e}^{2\pi \mathrm{i} S[g(\xi+\tau\eta)]/p}\right|,$$

其中

$$\left(\frac{\xi}{\kappa}\right) = \begin{cases} 1, & \text{如果 } \xi \text{ 是 } \kappa \text{ 中某个元的平方}, \\ -1, & \text{其他}. \end{cases}$$

如同第一种情形一样, 我们可以证明前 3 项中的每一项都为 $O(p^{m(2-\frac{2}{n})})$. 又有

$$\left|\sum_{\xi}\sum_{\eta}\left(\frac{\xi}{\kappa}\right)\left(\frac{\eta}{\kappa}\right) \mathrm{e}^{2\pi \mathrm{i} S[g(\xi+\tau\eta)]/p}\right|$$
$$= \left|\sum_{\xi}{}'\sum_{\eta}{}'\left(\frac{\xi}{\kappa}\right)\left(\frac{\xi\eta}{\kappa}\right) \mathrm{e}^{2\pi \mathrm{i} S[g(\xi(1+\tau\eta))]/p}\right| + O(p^m)$$
$$= \left|\sum_{\xi}{}'\sum_{\eta}{}'\left(\frac{\eta}{\kappa}\right) \mathrm{e}^{2\pi \mathrm{i} S[g(\xi(1+\tau\eta))]/p}\right| + O(p^m)$$
$$= O(p^{m(2-\frac{2}{n})})^{①},$$

这里 $\sum\limits_{t}{}'$ 表示 $t$ 过 $\kappa$ 中所有的非零元.

因此

$$\left|\sum_{x}\sum_{y} \mathrm{e}^{2\pi \mathrm{i} S[f(x,y)]/p}\right| = O(p^{m(2-\frac{2}{n})}).$$

2) 假设 $f(\alpha t+\alpha', \beta t+\beta') - f(\alpha', \beta')$ 的某 4 个系数的 Jacobi 行列式不恒等于 0. 设它为

$$J = J(\alpha, \alpha', \beta, \beta'),$$

又设关于 $\beta'$ 的最高次项的系数为 $J_0 = J_0(\alpha, \alpha', \beta)$.

显然, 有

$$(p^{3m} - O(p^{2m}))\left|\sum_{x}\sum_{y} \mathrm{e}^{2\pi \mathrm{i} S[f(x,y)]/p}\right|^{2n}$$

① 因为有限域的非零元关于乘法构成一个循环群, 所以, 假定 $\xi\eta \neq 0$, 容易证明 $\left(\frac{\xi}{\kappa}\right)\left(\frac{\eta}{\kappa}\right) = \left(\frac{\xi\eta}{\kappa}\right)$.

$$=\sum_{\alpha}\sum_{\alpha'}\sum_{\substack{\beta\\ \alpha J_0\neq 0\\ f_n(\alpha,\beta)\neq 0}}\left|\sum_{x}\sum_{\beta'}e^{2\pi i S[f(\alpha x+\alpha',\beta x+\beta')]/p}\right|^{2n}\quad (用引理 2)$$

$$=\sum_{\alpha}\sum_{\alpha'}\sum_{\substack{\beta\\ \alpha J_0\neq 0\\ f_n\neq 0}}\left|\sum_{\substack{\beta'\\ J\neq 0}}\sum_{x}e^{2\pi i S[f(\alpha x+\alpha',\beta x+\beta')]/p}\right.$$

$$\left.+\sum_{\substack{\beta'\\ J=0}}\sum_{x}e^{2\pi i S[f(\alpha x+\alpha',\beta x+\beta')]/p}\right|^{2n}$$

$$\leqslant 2^{2n-1}\sum_{\alpha}\sum_{\alpha'}\sum_{\substack{\beta\\ \alpha J_0\neq 0\\ f_n\neq 0}}\left|\sum_{\substack{\beta'\\ J\neq 0}}\sum_{x}e^{2\pi i S[f(\alpha x+\alpha',\beta x+\beta')]/p}\right|^{2n}$$

$$+2^{2n-1}\sum_{\alpha}\sum_{\alpha'}\sum_{\substack{\beta\\ \alpha J_0\neq 0\\ f_n\neq 0}}\left|\sum_{\substack{\beta'\\ J=0}}\sum_{x}e^{2\pi i S[f(\alpha x+\alpha',\beta x+\beta')]/p}\right|^{2n}$$

(用 Hölder 不等式)

$$\leqslant 2^{2n-1}p^{m(2n-1)}\sum_{\alpha}\sum_{\alpha'}\sum_{\substack{\beta\\ \alpha J_0\neq 0\\ f_n\neq 0}}\sum_{\substack{\beta'\\ J\neq 0}}\left|\sum_{x}e^{2\pi i S[f(\alpha x+\alpha',\beta x+\beta')]/p}\right|^{2n}$$

$$+O(p^{m(3+2n(1-\frac{1}{n}))})$$

(用 Hölder 不等式于第一项, 用引理 10 于第二项)

$$=p^{m(2n-1)}O\left(\sum_{A_n}\cdots\sum_{A_1}\left|\sum e^{2\pi i S[A_nx^n+\cdots+A_1x]/p}\right|^{2n}\right)$$

$$+O(p^{m(2n+1)})\quad (用引理 1)$$

$$=O(p^{m(4n-1)})\quad (用 (32) 式),$$

其中 $f_n(x,y)$ 表示 $f(x,y)$ 中的 $n$ 次项之和.

因此

$$\left|\sum_{x}\sum_{y}e^{2\pi i S[f(x,y)]/p}\right|^{2n}=O(p^{m(4n-4)}).$$

从而有

$$\sum_{x}\sum_{y}e^{2\pi i S[f(x,y)]/p}=O(p^{m(2-\frac{2}{n})}).$$

**附录**　前面的结果在条件 $n\geqslant 4$ 之下成立. 在附录中, 我们将证明, 对于 $n=2$ 和 3, 结果也成立. 我们甚至还有更强的结果, 即

**定理 2**　设 $f(x,y)$ 为 $\kappa$ 上的一个 3 次多项式, 它不等于一个单变量的 3 次多

项式, 则有

$$\sum_x \sum_y e^{\frac{2\pi i}{p} S[f(x,y)]} = O(p^{m(2-\frac{3}{4})}).$$

这个定理启发我们, 一些已经得到的结果可以进一步地改进, 而这确实是可能的.

**引理 11** 令

$$\phi = \sum_{i=1}^{r} \sum_{j=1}^{r} a_{i,j} x_i x_j \quad (a_{i,j} = a_{j,i})$$

为整系数的二次型. 设 $p \nmid \Delta, \Delta = |a_{i,j}|$. 则有

$$S = \sum_{x_1=1}^{p} \cdots \sum_{x_r=1}^{p} e^{\frac{2\pi i}{p}\phi} = i^{r(\frac{p-1}{2})^2} p^{\frac{r}{2}} \left(\frac{\Delta}{p}\right).$$

**证明** 考虑由 $\bmod p$ 的剩余类所构成的域 $\Pi$. 众所周知, 存在着 $\Pi$ 上的一个非奇异变换

$$x_i = \sum_{j=1}^{r} c_{i,j} y_j, \quad i = 1, \cdots, r,$$

它将 $\phi$ 变成标准形式 $\sum_{i=1}^{r} \lambda_i y_i^2$. 因为

$$|c_{i,j}| \not\equiv 0(p),$$

所以, 易见当 $x_i (i = 1, \cdots, r)$ 独立地过 $\bmod p$ 的完全剩余系时, $y_i (i = 1, \cdots, r)$ 亦然. 因此

$$\begin{aligned} S &= \sum_{y_1=1}^{p} \cdots \sum_{y_r=1}^{p} e^{\frac{2\pi i}{p}(\lambda_1 y_1^2 + \cdots + \lambda_r y_r^2)} \\ &= \sum_{y_1=1}^{p} e^{\frac{2\pi i}{p}\lambda_1 y_1^2} \cdots \sum_{y_r=1}^{p} e^{\frac{2\pi i}{p}\lambda_r y_r^2} \\ &= i^{r(\frac{p-1}{2})^2} p^{\frac{r}{2}} \left(\frac{\lambda_1 \cdots \lambda_r}{p}\right). \end{aligned}$$

因为 $\lambda_1 \cdots \lambda_r = \Delta |c_{i,j}|^2$, 所以, 我们可得引理.

**引理 12**[①] 如果 $a$ 属于 $\kappa, a \neq 0$, 则有

$$\sum_x e^{2\pi i S[ax^2]/p} = \varepsilon i^{m(\frac{p-1}{2})^2} p^{\frac{m}{2}} \left(\frac{a}{\kappa}\right),$$

① 这个公式是 Davenport 和 Hasse 的一个结果的推论. 然而, 我们不借助于他们的结果而给出了本引理的详细证明, 因而本文是自封闭的.

其中 $\left(\frac{a}{\kappa}\right)=+1$ 或 $-1$, 依方程 $x^2=u$ 在 $\kappa$ 中有没有解而定, 而 $\varepsilon(=\pm1)$ 仅依赖于域 $\kappa$.

**证明** 1) 假设 $\left(\frac{a}{\kappa}\right)=1$. 不失一般性, 我们可设 $a=1$. 因为 $\kappa$ 中的每个元 $x$ 都可写作

$$x=a_0+a_1\theta+\cdots+a_{m-1}\theta^{m-1},\quad a_i\in\Pi,$$

所以, 我们有

$$\sum_x \mathrm{e}^{2\pi\mathrm{i}S[x^2]/p}=\sum_{a_0=1}^{p}\cdots\sum_{a_{m-1}=1}^{p}e_p\left(\sum_{r=0}^{2(m-1)}\sum_{i+j=r}a_ia_jS[\theta^r]\right),$$

这里 $e_p(u)=\mathrm{e}^{2\pi\mathrm{i}u/p}$.

$\sum_{r=0}^{2(m-1)}\sum_{i+j=r}S[\theta^r]a_ia_j$ 的行列式为

$$|S[\theta^{i+j-2}]|=\begin{vmatrix} m & s_1 & \cdots & s_{m-1}\\ s_1 & s_2 & \cdots & s_m\\ \vdots & \vdots & & \vdots\\ s_{m-1} & s_m & \cdots & s_{2(m-1)}\end{vmatrix},$$

其中 $s_\nu=\theta^\nu+\theta_1^\nu+\cdots+\theta_{m-1}^\nu(\nu=1,\cdots,m-1),\theta_1,\cdots,\theta_{m-1}$ 为 $\theta$ 的共轭元. 因为 $\theta,\theta_1,\cdots,\theta_{m-1}$ 互不相同, 所以

$$\begin{aligned}|S[\theta^{i+j-2}]|=&\begin{vmatrix} 1 & 1 & \cdots & 1\\ \theta & \theta_1 & \cdots & \theta_{m-1}\\ \vdots & \vdots & & \vdots\\ \theta^{m-1} & \theta_1^{m-1} & \cdots & \theta_{m-1}^{m-1}\end{vmatrix}\\ &\times\begin{vmatrix} 1 & \theta & \cdots & \theta^{m-1}\\ 1 & \theta_1 & \cdots & \theta_1^{m-1}\\ \vdots & \vdots & & \vdots\\ 1 & \theta_{m-1} & \cdots & \theta_{m-1}^{m-1}\end{vmatrix}\\ =&\prod_{0<i<j\leqslant m-1}(\theta_i-\theta_j)^2\\ =&A\neq0.\end{aligned}$$

因为 $p\nmid A$, 所以, 由引理 11 知

$$\sum_x \mathrm{e}^{2\pi\mathrm{i}S[x^2]/p}=\mathrm{i}^{m(\frac{p-1}{2})^2}p^{\frac{m}{2}}\left(\frac{A}{P}\right),$$

即

$$\sum_x e^{2\pi i S[ax^2]/p} = \varepsilon i^{m(\frac{p-1}{2})^2} p^{\frac{m}{2}} \left(\frac{a}{\kappa}\right).$$

因为左边和 $i^{m(\frac{p-1}{2})^2} p^{\frac{m}{2}} \left(\frac{a}{\kappa}\right)$ 都与生成元 $\theta$ 的选取无关, 所以, $\varepsilon$ 仅依赖于 $\kappa$.

2) 现在假设 $\left(\frac{a}{\kappa}\right) = -1$. 当 $x$ 过 $\kappa$ 中所有的非零元时, $x^2$ 过所有非零的平方, 而 $ax^2$ 过所有非零的非平方. 因此

$$\sum_x e^{2\pi i S[ax^2]/p} + \sum_x e^{2\pi i S[x^2]/p} = 2\sum_x e^{2\pi i S[x]/p} = 0.$$

从而有

$$\sum_x e^{2\pi i S[ax^2]/p} = -\sum_x e^{2\pi i S[x^2]/p} = \varepsilon i^{m(\frac{p-1}{2})^2} \left(\frac{a}{\kappa}\right).$$

**引理 13** 设

$$\phi = ax^2 + 2hxy + by^2 + 2fx + 2gy + c$$

为 $\kappa$ 上的多项式, $\Delta = h^2 - ab \neq 0$. 则有

$$S = \sum_x \sum_y e^{2\pi i S[\phi]/p} = \left(\frac{\Delta}{\kappa}\right) p^m e_p\left(S\left[c + \frac{bf^2 + ag^2 - 2fgh}{\Delta}\right]\right),$$

其中 $e_p(u) = e^{2\pi i u/p}$.

**证明** 我们设 $a \neq 0$. 记

$$X = x + \frac{h}{a}y + \frac{f}{a}, \quad Y = y - \frac{ag - hf}{\Delta}.$$

由引理 12 可得

$$\begin{aligned} S =& \sum_x \sum_y e_p\left(S\left[aX^2 - \frac{\Delta}{a}Y^2 + c + \frac{bf^2 + ag^2 - 2fgh}{\Delta}\right]\right) \\ =& \varepsilon \left(\frac{a}{\kappa}\right) i^{m(\frac{p-1}{2})^2} p^{\frac{m}{2}} \varepsilon \left(\frac{-\Delta/a}{\kappa}\right) i^{m(\frac{p-1}{2})^2} p^{\frac{m}{2}} \\ & \cdot e_p\left(S\left[c + \frac{bf^2 + ag^2 - 2fgh}{\Delta}\right]\right), \end{aligned}$$

这里用到了

$$\begin{aligned} & ax^2 + 2hxy + by^2 + 2fx + 2gy + c \\ =& a\left(x + \frac{h}{a}y + \frac{f}{a}\right)^2 - \frac{\Delta}{a}\left(y - \frac{ag - hf}{\Delta}\right)^2 + c + \frac{bf^2 + ag^2 - 2fgh}{\Delta}. \end{aligned}$$

因为有限域中的非零元对于乘法构成一个循环群, 所以, 易证

$$\left(\frac{\xi}{\kappa}\right)\left(\frac{\eta}{\kappa}\right)=\left(\frac{\xi\eta}{\kappa}\right),\quad \left(\frac{-1}{\kappa}\right)=(-1)^{\frac{p^m-1}{2}}=(-1)^{m(\frac{p-1}{2})}.$$

因此

$$S=\left(\frac{\Delta}{\kappa}\right)p^m e_p\left(S\left[c+\frac{bf^2+ag^2-2fgh}{\Delta}\right]\right).$$

同样的结果对于 $b\neq 0$ 也成立. 现在设 $a=0,b=0$. 于是, $h\neq 0$ 且

$$\begin{aligned}S&=\sum_x\sum_y e_p(S[2hxy+2fx+2gy+c])\\&=\sum_y e_p(S[2gy+c])\sum_x e_p(S[(2hy+2f)x])\\&=p^m\sum_{2hy+2f=0}e_p(S[2gy+c])\\&=p^m e_p\left(S\left[c-\frac{2gf}{h}\right]\right).\end{aligned}$$

**定理的证明**　令

$$S=\sum_x\sum_y e_p(S[f(x,y)])$$

和

$$\begin{aligned}f(x,y)=&a_0x^3+a_1x^2y+a_2xy^2+a_3y^3+b_0x^2\\&+b_1xy+b_2y^2+c_0x+c_1y.\end{aligned}$$

首先, 假设除去一个常数因子外, $a_0x^3+a_1x^2y+a_2xy^2+a_3y^3$ 为一个完全立方. 不失一般性, 我们可设 $a_1=a_2=a_3=0$. 如若不然, 我们用一个简单的变换, 可以将 $f(x,y)$ 约化为这种形式. 于是

$$S=\sum_x\sum_y e_p(S[a_0x^3+b_0x^2+b_1xy+b_2y^2+c_0x+c_1y]).$$

如果 $b_2=0$, 则 $b_1$ 和 $c_1$ 不能同时为 0, 因此,

$$\begin{aligned}S&=\sum_{\substack{x\\b_1x+c_1=0}}\sum_y e_p(S[a_0x^3+b_0x^2+c_0x+(b_1x+c_1)y])\\&=\begin{cases}O(p^m),&\text{当 } b_1\neq 0 \text{ 时},\\0,&\text{当 } b_1=0 \text{ 时}.\end{cases}\end{aligned}$$

如果 $b_2 \neq 0$, 不失一般性, 我们可设 $b_1 = 0$. 如果 $b_1 \neq 0$, 我们用变换 $X = x, Y = b_1x + b_2y$, 可将 $f(x,y)$ 约化为一个没有 $xy$ 项的多项式. 因此, 由引理 10 和 12 知

$$\begin{aligned}S &= \sum_x e_p(S[a_0x^3 + b_0x^2 + c_0x]) \sum_y e_p(S[b_2y^2 + c_1y]) \\ &= O(p^{m(1-\frac{1}{3})})O(p^{\frac{m}{2}}) = O(p^{m(2-\frac{5}{6})}) \\ &= O(p^{m(2-\frac{3}{4})}).\end{aligned}$$

其次, 假设 $a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3$ 不为一个常数乘上一个完全立方. 则有

$$\begin{aligned}|S|^2 =& \sum_{x_1}\sum_{x_2}\sum_{y_1}\sum_{y_2} e_p(S[a_0(x_1^3 - x_2^3) + a_1(x_1^2y_1 - x_2^2y_2) \\ &+ a_2(x_1y_1^2 - x_2y_2^2) + a_3(y_1^3 - y_2^3) + b_0(x_1^2 - x_2^2) \\ &+ b_1(x_1y_1 - x_2y_2) + b_2(y_1^2 - y_2^2) + c_0(x_1 - x_2) + c_1(y_1 - y_2)]).\end{aligned}$$

令

$$\begin{aligned}x_1 - x_2 = 2\xi_1, \quad x_1 + x_2 = 2\xi_2, \\ y_1 - y_2 = 2\eta_1, \quad y_1 + y_2 = 2\eta_2.\end{aligned}$$

因为

$$x_1^3 - x_2^3 = 2\xi_1(3\xi_2^2 + \xi_1^2), \quad x_1^2y_1 - x_2^2y_2 = 2\eta_1(\xi_1^2 + \xi_2^2) + 4\xi_1\xi_2\eta_2, \text{等等},$$

所以, 我们有

$$\begin{aligned}|S|^2 =& \sum_{\xi_1}\sum_{\eta_1}\sum_{\xi_2}\sum_{\eta_2} e_p(S[2a_0\xi_1(3\xi_2^2 + \xi_1^2) + 2a_1(\eta_1(\xi_1^2 + \xi_2^2) \\ &+ 2\xi_1\xi_2\eta_2) + 2a_2(\xi_1(\eta_1^2 + \eta_2^2) + 2\eta_1\eta_2\xi_2) + 2a_3\eta_1(3\eta_2^2 + \eta_1^2) \\ &+ 4b_0\xi_1\xi_2 + 2b_1(\xi_1\eta_2 + \xi_2\eta_1) + 4b_2\eta_1\eta_2 + 2c_0\xi_1 + 2c_1\eta_1]) \\ =& \sum_{\xi_1}\sum_{\eta_1}\sum_{\xi_2}\sum_{\eta_2} e_p(S[\phi]),\end{aligned} \tag{33}$$

其中

$$\begin{aligned}\phi =& (6a_0\xi_1 + 2a_1\eta_1)\xi_2^2 + 2(2a_1\xi_1 + 2a_2\eta_1)\xi_2\eta_2 \\ &+ (2a_2\xi_1 + 6a_3\eta_1)\eta_2^2 + 2(2b_0\xi_1 + b_1\eta_1)\xi_2 \\ &+ 2(b_1\xi_1 + 2b_2\eta_1)\eta_2 + 2a_0\xi_1^3 + 2a_1\xi_1^2\eta_1 + 2a_2\xi_1\eta_1^2 + 2a_3\eta_1^3 \\ &+ 2c_0\xi_1 + 2c_1\eta_1.\end{aligned}$$

令

$$\Delta = \Delta(\xi, \eta) = (2a_1\xi_1 + 2a_2\eta_1)^2 - (6a_0\xi_1 + 2a_1\eta_1)(2a_2\xi_1 + 6a_3\eta_1)$$

$$=4(a_1^2-3a_0a_2)\xi_1^2+4(a_1a_2-9a_0a_3)\xi_1\eta_1+4(a_2^2-3a_1a_3)\eta_1^2.$$

$\Delta(\xi,\eta)$ 不恒等于 0. 如若不然, 我们一定有

$$a_1^2=3a_0a_2,\quad a_1a_2=9a_0a_3,\quad a_2^2=3a_1a_3.$$

如果 $a_0=0$, 则 $a_1=0, a_2=0$. 于是, $a_0x^3+a_1x^2y+a_2y^2+a_3y^3=a_3y^3$, 但这与我们的假设相矛盾. 如果 $a_0\neq 0$, 则有

$$a_2=\frac{a_1^2}{3a_0},\quad a_3=\frac{a_1a_2}{9a_0}=\frac{a_1^3}{27a_0^3}.$$

于是

$$a_0x^3+a_1x^2y+a_2xy^2+a_3y^3=a_0\left(x+\frac{a_1}{3a_0}y\right)^3,$$

但这也与我们的假设相矛盾. 于是, 显然

$$\Delta=\Delta(\xi,\eta)=0$$

有 $O(p^m)$ 个解.

由 (33) 式,

$$\begin{aligned}|S|^2&=\sum_{\xi_1}\sum_{\substack{\eta_1\\ \Delta\neq 0}}\sum_{\xi_2}\sum_{\eta_2}e_p(S[\phi])+\sum_{\xi_1}\sum_{\substack{\eta_1\\ \Delta=0}}\sum_{\xi_2}\sum_{\eta_2}e_p(S[\phi])\\&=S_1+S_2.\end{aligned}$$

由引理 13 知,

$$\begin{aligned}S_1=&p^m\sum_{\xi_1}\sum_{\substack{\eta_1\\ \Delta\neq 0}}\left(\frac{\Delta}{\kappa}\right)e_p\bigg(S\bigg[2a_0\xi_1^3+2a_1\xi_1^2\eta_1+2a_2\xi_1\eta_1^2\\&+2c_0\xi_1+2c_1\eta_1+\frac{H(\xi_1,\eta_1)}{\Delta(\xi_1,\eta_1)}\bigg]\bigg)\\=&p^m\sum_{\xi_1}\sum_{\substack{\eta_1\\ \xi_1\,\Delta\neq 0}}\left(\frac{\Delta}{\kappa}\right)e_p\bigg(S\bigg[2a_0\xi_1^3+2a_1\xi_1^2\eta_1+2a_2\xi_1\eta_1^2\\&+2c_0\xi_1+2c_1\eta_1+\frac{H(\xi_1,\eta_1)}{\Delta(\xi_1,\eta_1)}\bigg]\bigg)+O(p^{2m}),\end{aligned}$$

其中

$$\begin{aligned}H=&H(\xi,\eta)=(2a_2\xi_1+6a_3\eta_1)(2b_0\xi_1+b_1\eta_1)^2\\&+(6a_0\xi_1+2a_1\eta_1)(b_1\xi_1+2b_2\eta_1)^2\\&-2(2b_0\xi_1+b_1\eta_1)(b_1\xi_1+2b_2\eta_1)(2a_1\xi_1+2a_2\eta_1).\end{aligned}$$

取 $\xi_1=\xi,\eta_1=\xi\eta$, 我们有

$$S_1 = p^m \sum_{\xi} \sum_{\substack{\eta \\ \Delta(1,\eta)\neq 0}} \left(\frac{\Delta(1,\eta)}{\kappa}\right) e_p\Big(S\Big[(2a_0+2a_1\eta+2a_2\eta^2+2a_3\eta^3)\xi^3 + \left(2c_0+2c_1\eta+\frac{H(1,\eta)}{\Delta(1,\eta)}\right)\xi\Big]\Big) + O(p^{2m}), \tag{34}$$

这里用到关于 $\xi=0$ 的项的求和为 $O(p^{2m})$.

如果 $2c_0+2c_1\eta+\dfrac{H(1,\eta)}{\Delta(1,\eta)}$ 恒等于 0, 则我们有

$$\begin{aligned}
|S_1|^2 \leqslant & 2p^{2m}p^m \sum_{\substack{\eta \\ \Delta(1,\eta)\neq 0}} \left|\sum_{\xi} e_p(S[(2a_0+2a_1\eta+2a_2\eta^2+2a_3\eta^3)\xi^3])\right|^2 + O(p^{4m}) \\
= & O\left(p^{3m}\sum_a\left|\sum_\xi e_p(S[a\xi^3])\right|^2\right)+O(p^{4m}) \\
= & O\left(p^{3m}\sum_{\xi_1}\sum_{\xi_2}\sum_a e_p(S[a(\xi_1^3-\xi_2^3)])\right)+O(p^{4m}) \\
= & O\left(p^{3m}\sum_{\xi_1}\sum_{\substack{\xi_2 \\ \xi_1^3=\xi_2^3}} p^m\right)+O(p^{4m}) \\
= & O(p^{5m}).
\end{aligned}$$

因此

$$S_1 = O(p^{\frac{5m}{2}}). \tag{35}$$

如果 $2c_0+2c_1\eta+\dfrac{H(1,\eta)}{\Delta(1,\eta)}$ 不恒等于 0, 则方程组

$$c^3(2a_0+2a_1\eta+2a_2\eta^2+2a_3\eta^3)=A, \tag{36}$$

$$c\left(2c_0+2c_1\eta+\frac{H(1,\eta)}{\Delta(1,\eta)}\right)=B, \quad B\neq 0$$

有 $O(1)$ 个解. 事实上, 通过消去 $c$, 我们有

$$B^3(2a_0+2a_1\eta+2a_2\eta^2+2a_3\eta^3)=A\left(2c_0+2c_1\eta+\frac{H(1,\eta)}{\Delta(1,\eta)}\right)^3.$$

因为 $2a_0+2a_1\eta+2a_2\eta^2+2a_3\eta^3$ 不为一个常数乘上一个完全立方, 所以, 上面的等式不是恒等式. 因而, 它关于 $\eta$ 有 $O(1)$ 个解. 而 $c$ 是由 (36) 式中的第二个等式唯一决定的, 因此, (36) 式关于 $\eta,c$ 有 $O(1)$ 个解.

由 (34) 式,

$$\begin{aligned}S_1 =&p^m\sum_{\xi}\sum_{\substack{\eta\\ \Delta(1,\eta)\neq 0}}\left(\frac{\Delta(1,\eta)}{\kappa}\right)e_p\Big(S\Big[(2a_0+2a_1\eta\\&+2a_2\eta^2+2a_3\eta^3)\xi^3+\left(2c_0+2c_1\eta+\frac{H(1,\eta)}{\Delta(1,\eta)}\right)\xi\Big]\Big)+O(p^{2m}),\\&2c_0+2c_1\eta+\frac{H(1,\eta)}{\Delta(1,\eta)}\neq 0.\end{aligned}$$

因此

$$\begin{aligned}|S_1|^4 \leqslant&8p^{4m+3m}\sum_{\substack{\eta\\ \Delta(1,\eta)\neq 0}}\Big|\sum_{\xi}e_p\Big(S\Big[(2a_0+2a_1\eta\\&+2a_2\eta^2+2a_3\eta^3)\xi^3+\left(2c_0+2c_1\eta+\frac{H(1,\eta)}{\Delta(1,\eta)}\right)\xi\Big]\Big)\Big|^4+O(p^{8m}),\\&2c_0+2c_1\eta+\frac{H(1,\eta)}{\Delta(1,\eta)}\neq 0.\end{aligned}$$

从而, 由引理 11 可得

$$\begin{aligned}(p^m-1)|S_1|^4 \leqslant&8p^{7m}\sum_{\substack{c\\ c\neq 0}}\sum_{\substack{\eta\\ \Delta(1,\eta)\neq 0}}\Big|\sum_{\xi}e_p\Big(S\Big[c^3(2a_0+2a_1\eta+2a_2\eta^2+2a_3\eta^3)\xi^3\\&+c\left(2c_0+2c_1\eta+\frac{H(1,\eta)}{\Delta(1,\eta)}\right)\xi\Big]\Big)\Big|^4+O(p^{9m})\\&\left(2c_0+2c_1\eta+\frac{H(1,\eta)}{\Delta(1,\eta)}\neq 0\right)\\=&O\left(p^{7m}\sum_{A}\sum_{B}\Big|\sum_{\xi}e_p(S[A\xi^3+B\xi])\Big|^4\right)+O(p^{9m})\\=&O(p^{7m}p^{4m})\\=&O(p^{11m}).\end{aligned}$$

由此可得

$$S_1=O(p^{\frac{5m}{2}}).\tag{37}$$

现在让我们来估计 $S_2$. 因为 $\Delta(\xi,\eta)=0$ 有 $O(p^m)$ 个解, 所以, 我们有

$$S_2=O\Big(p^m\max_{\substack{\Delta(\xi_1,\eta_1)=0\\ \xi_1\neq 0或\eta_1\neq 0}}\sum_{\xi_2}\sum_{\eta_2}e_p(S[\phi])+p^{2m}\Big).$$

因为 $a_0+a_1\eta+a_2\eta^2+a_3\eta^3$ 不为一个常数乘上一个完全立方, 所以, $\phi$ 中 $\xi_2^2,\xi_2\eta_2,\eta_2^2$ 的系数不能同时为 0, 除非 $\xi_1=\eta_1=0$. 因为 $\Delta=0$, 所以, $\xi_2^2$ 和 $\eta_2^2$ 的系数不能全为 0. 因此, 由引理 12 知

$$S_2 = O(p^m p^m p^{\frac{m}{2}}) = O(p^{\frac{5m}{2}}). \tag{38}$$

由 (35) 式 (或 (37) 式) 和 (38) 式, 我们有

$$|S|^2 = S_1 + S_2 = O(p^{\frac{5m}{2}}).$$

从而可得

$$S = O(p^{\frac{5m}{4}}) = O(p^{m(2-\frac{3}{4})}).$$

(潘承彪 译)

# Vinogradov 中值定理的改进与应用[①]

华罗庚

## 1. 导　　言

在 1940 年, 我证明了[②] Vinogradov 关于 Weyl 和的估计主要依赖于我称之为 "Vinogradov 中值定理" 的一个结果. 本文的目的为改进这个中值定理. 由于 Vinogradov 方法似乎已达到了最后阶段, 所以任何关于指数常数的改进都是值得考虑的. 更确切地说, 在本文中, 我将建立一个中值公式, 用它我们可以得到关于 Waring 问题、素数分布等问题更为精确的结果. 这里用的方法似乎比 Vinogradov 原来的方法要简单得多.

我们证明的 Vinogradov 中值定理的形式为下定理:

**定理 1**　命 $P$ 与 $T$ 为整数及 $P \geqslant 2$, 及命

$$f(x) = \alpha_k x^k + \cdots + \alpha_1 x, \tag{1}$$

$$G_k = G_k(P) = \sum_{T<x\leqslant T+P} \mathrm{e}^{2\pi \mathrm{i} f(x)}. \tag{2}$$

则当

$$s \geqslant \frac{1}{4}k(k+1) + lk \tag{3}$$

时, 我们有

$$\int_0^1 \cdots \int_0^1 |G_k(P)|^{2s} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_2 \leqslant (7s)^{4sl} (\log P)^{2l} P^{2s-\frac{1}{2}k(k+1)+\delta}, \tag{4}$$

此处

$$\delta = \frac{1}{2}k(k+1)(1-1/k)^l. \tag{5}$$

从算术上讲, (4) 中的积分等于方程组

$$x_1^h + \cdots + x_s^h = y_1^h + \cdots + y_s^h \quad (1 \leqslant h \leqslant k) \tag{6}$$

---

① 1948 年 7 月 21 日收到. 发表于 *Quart. J. Math.*, 1949, 20: 48–61.

② 华罗庚. 堆垒素数论. 这本书已于 1940 年由苏联科学院接受出版, 但由于战争关系而延迟了出版.

的解数, 此处

$$T < x_i, y_i \leqslant T + P.$$

置 $X_i = x_i - T, Y_i = y_i - T$, 则由 (6) 得

$$\sum_{i=1}^{s}(X_i + T)^h = \sum_{i=1}^{s}(Y_i + T)^h \quad (1 \leqslant h \leqslant k). \tag{7}$$

将 $h$ 次幂展开, 我们见到方程组 (7) 等价于

$$\sum_{i=1}^{s} X_i^h = \sum_{i=1}^{s} Y_i^h \quad (1 \leqslant h \leqslant k), \tag{8}$$

此处 $0 < X_i, Y_i \leqslant P$. 这表明了 (4) 的左端的确独立于 $T$.

由于 Vinogradov 的文章与我的书都是用俄文发表的. 所以本文将从头讲起.

## 2. 引　理

**引理 1**　命 $Q = RH, R > 1, H > 1$ 及命 $g_1, \cdots, g_k$ 为适合

$$1 < g_1 < g_2 < \cdots < g_k \leqslant H, \quad g_\nu - g_{\nu-1} > 1 \tag{9}$$

之整数. 对于每一个 $\nu(1 \leqslant \nu \leqslant k)$, 命 $x_\nu$ 为一个位于区间

$$-\omega + (g_\nu - 1)R < x_v \leqslant -\omega + g_\nu R \quad (0 \leqslant \omega \leqslant Q) \tag{10}$$

中的变数. 这种 $x_1, \cdots, x_k$ 整数组, 使

$$x_1^h + \cdots + x_k^h \tag{11}$$

之值分别位于长度不超过 $Q^{h-1}(1 \leqslant h \leqslant k)$ 之区间之个数小于或等于

$$(2kH)^{\frac{1}{2}k(k-1)}. \tag{12}$$

**证明**　命 $x_1, \cdots, x_k$ 与 $y_1, \cdots, y_k$ 为满足引理要求的两组整数; 命

$$s_h = \sum_{\nu=1}^{k} x_\nu^h, \quad s'_h = \sum_{\nu=1}^{k} y_\nu^h,$$

及命 $\sigma_h$ 与 $\sigma'_h$ 分别表示 $x_1, \cdots, x_k$ 与 $y_1, \cdots, y_k$ 的 $h$ 次初等对称函数, 则由 (10) 可知

$$|s_h| \leqslant \sum_{\nu=1}^{k} |x_\nu|^h \leqslant kQ^h, \quad |s'h| \leqslant kQ^h \tag{13}$$

与

$$|\sigma_h| \leqslant \binom{k}{h} Q^h, \quad |\sigma_h'| \leqslant \binom{k}{h} Q^h. \tag{14}$$

由假定得

$$|s_h - s_h'| \leqslant Q^{h-1} \quad (1 \leqslant h \leqslant k). \tag{15}$$

由 (15), 我们将证明

$$|\sigma_h - \sigma_h'| \leqslant \frac{3}{4}(2kQ)^{h-1}, \quad 2 \leqslant h \leqslant k, \tag{16}$$

从而

$$|\sigma_h - \sigma_h'| \leqslant (2kQ)^{h-1}, \quad 1 \leqslant h \leqslant k. \tag{17}$$

由于 $\sigma_2 = \frac{1}{2}(s_1^2 - s_2)$, 所以由 (13) 可知

$$\begin{aligned} |\sigma_2 - \sigma_2'| &\leqslant \frac{1}{2}\{|s_1 - s_1'|(|s_1| + |s_1'|) + 2|s_2 - s_2'|\} \\ &\leqslant \frac{1}{2}(2k+1)Q \leqslant \frac{3}{4}(2kQ), \end{aligned} \tag{18}$$

因此 (16) 对于 $h = 2$ 成立. 我们用归纳法并假定 (16) 对于 $2 \leqslant h \leqslant t-1$ 成立. 则由 (13), (14), (15) 与 (16) 可知, 当 $1 \leqslant \nu \leqslant t-1$ 时

$$\begin{aligned} |\sigma_\nu s_{t-\nu} - \sigma_\nu' s_{t-\nu}'| &\leqslant |\sigma_\nu - \sigma_\nu'||s_{t-\nu}| + |\sigma_\nu'||s_{t-\mu} - s_{t-\nu}'| \\ &\leqslant \left\{(2k)^\nu k + \binom{k}{\nu}\right\} Q^{t-1} \\ &\leqslant \left(1 + \frac{1}{\nu!}\right)(2k)^{\nu-1} k Q^{t-1}. \end{aligned} \tag{19}$$

由对称函数一条熟知的定理得

$$s_t - \sigma_1 s_{t-1} + \sigma_2 s_{t-2} - \cdots + (-1)^t t\sigma_t = 0 \tag{20}$$

与

$$s_t' - \sigma_1' s_{t-1}' + \sigma_2' s_{t-2}' - \cdots + (-1)^t t\sigma_t' = 0. \tag{21}$$

联合 (19), (20) 与 (21) 得

$$\begin{aligned} |\sigma_t - \sigma_t'| &\leqslant \frac{1}{t}\left(1 + 2k + \frac{3}{2}k\sum_{\nu=2}^{t-1}(2k)^{\nu-1}\right) Q^{t-1} \\ &\leqslant \frac{1}{2}\left[1 + 2k + \frac{3}{2}k\{(2k)^{t-1} - 2k\}/(2k-1)\right] Q^{t-1} \\ &\leqslant \frac{1}{2}\left\{1 + \frac{1}{2}k + \frac{3}{2}k(2k)^{t-1}/(2k-1)\right\} Q^{t-1} \end{aligned}$$

$$\leqslant \frac{3}{4}(2k)^{t-1}Q^{t-1}. \tag{22}$$

由于 $2k/(2k-1) \leqslant \frac{4}{3}$, 所以当 $|X| \leqslant Q$ 时得

$$\begin{aligned}
&|(X-x_1)\cdots(X-x_k)-(X-y_1)\cdots(X-y_k)| \\
\leqslant &\sum_{h=1}^{k} |\sigma_h - \sigma_h'||X|^{k-h} \\
\leqslant &\left\{1+\frac{3}{4}\sum_{h=2}^{k}(2k)^{h-1}\right\}Q^{k-1} \\
\leqslant &\left\{1+\frac{6k}{4(2k-1)}\{(2k)^{k-1}-1\}\right\}Q^{k-1} \\
\leqslant &(2kQ)^{k-1},
\end{aligned} \tag{23}$$

但是当 $\nu = 1, 2, \cdots, k-1$ 时, $|y_k - x_\nu| \geqslant R$, 所以若在 (23) 中置 $X = y_k$. 则得

$$R^{k-1}|y_k - x_k| \leqslant (2kQ)^{k-1}.$$

因此适合我们定理要求的 $x_k$ 的个数不超过 $(2kQ)^{k-1}$. 其次, 对于固定的 $x_k$, 数

$$x_1^h + \cdots + x_{k-1}^h \quad (1 \leqslant h \leqslant k-1) \tag{24}$$

分别位于长度最多为 $Q^{h-1}(1 \leqslant h \leqslant k-1)$ 的区间中, 这就归结到引理的准确形式, 其中用 $k-1$ 代替 $k$. 当 $k=1$ 时, 引理显然成立, 我们假定它对于较小的 $k$ 成立; 则满足条件 (24) 的整数 $x_1, \cdots, x_{k-1}$ 的集合个数不超过

$$\{2(k-1)H\}^{\frac{1}{2}(k-1)(k-2)}.$$

所以满足条件 (11) 的整数组的个数小于或等于

$$\{2(k-1)H\}^{\frac{1}{2}(k-1)(k-2)}(2kH)^{k-1} \leqslant (2kH)^{\frac{1}{2}k(k-1)}.$$

**引理 2** 命 $c \geqslant 1$, 则在引理 1 的同样假定下, 整数组 $x_1, \cdots, x_k$ 使

$$x_1^h + \cdots + x_k^h \quad (1 \leqslant h \leqslant k)$$

分别落在长度不超过 $cQ^{(1-\frac{1}{k})h}(1 \leqslant h \leqslant k)$ 之区间中者之个数不超过

$$(2c)^k(2kH)^{\frac{1}{2}k(k-1)}Q^{\frac{1}{2}(k-1)}. \tag{25}$$

**证明** 我们将第 $h$ 个区间分成

$$\{cQ^{h(1-1/k)}/Q^{h-1}\}+1$$

部分并应用引理 1. 由于

$$\prod_{h=1}^{k}\{(cQ^{h(1-1/k)}/Q^{h-1})+1\}\leqslant\prod_{h=1}^{k}(2cQ^{h(1-1/k)-(h-1)})=(2c)^kQ^{\frac{1}{2}(k-1)},$$

所以最多只有 $(2c)^kQ^{\frac{1}{2}(k-1)}$ 个子区间的集合, 其中每一集合均适合引理 1 的假设. 所以每一集合中最多只有 $(2kH)^{\frac{1}{2}k(k-1)}$ 个解, 引理证完.

**引理 3** 若整数集合 $(g_1,\cdots,g_b)$, 此处 $1\leqslant g_\nu\leqslant H$, 中至少有 $k$ 个, 例如 $g_{j_1},\cdots,g_{j_k}$ 满足

$$g_{j_{\nu+1}}-g_{j_\nu}>1\quad(1\leqslant\nu\leqslant k-1),\tag{26}$$

则称这一集合为 "佳位" 集, 非佳位集的个数最多为

$$b!3^bH^{k-1}.\tag{27}$$

**证明** 我们按照 $g_1,\cdots,g_b$ 的大小, 将它们排列成递增序列

$$1\leqslant g_1'\leqslant g_2'\leqslant\cdots\leqslant g_b',\tag{28}$$

并置 $f_\nu=g_{\nu+1}'-g_\nu'$. 若这一集合是非佳位的, 则至多只有 $k-2$ 个 $f$ 满足 $f_\nu>1$.

现在考虑正好有 $\sigma(0\leqslant\sigma\leqslant k-2)$ 个 $f$ 满足 $f_\nu>1$ 之诸集合, 这 $\sigma$ 个 $f$ 的不同位置之个数为 $\binom{b-1}{\sigma}$. 由于 $0\leqslant f_\nu\leqslant H-1$ 及 $1\leqslant g_1'\leqslant H$, 所以不同集合的个数最多为

$$\binom{b-1}{\sigma}H^{\sigma+1}2^{b-1-\sigma},$$

因此非佳位集合的总数

$$\leqslant\sum_{\sigma=0}^{k-2}\binom{b-1}{\sigma}H^{\sigma+1}2^{b-1-\sigma}\leqslant(1+2)^{b-1}H^{k-1}\leqslant3^bH^{k-1}.$$

由于对应于 $(g_1',\cdots,g_b')$ 的集合 $(g_1,\cdots,g_b)$ 的个数为 $b!$ 故得引理.

## 3. 递推公式

**定理 2** 命 $b$ 为一个整数 $\geqslant\frac{1}{4}k(k+1)+k$ 及 $\eta$ 为不超过

$$\frac{1}{k}\log Q/\log 2\tag{29}$$

的最大整数, 则

$$\int_0^1\cdots\int_0^1|C_k(Q)|^{2b}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k$$

$$\leqslant (7b)^{4b}\max(1,\eta^2)Q^{2k-\frac{1}{2}(k+1)+2(b-k)/k}$$
$$\times\int_0^1\cdots\int_0^1|C_k(Q^{1-1/k})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k. \tag{30}$$

**证明** (i) 在定理 1 中, 我们定义

$$C_k(Q)=\sum_{T<x\leqslant T+Q}\mathrm{e}^{2\pi\mathrm{i}f(x)}.$$

由那里的注记可知不失一般性, 我们可以在今后假定 $T=0$. 假定 $\eta\geqslant 2$ 及 $s$ 为一个满足 $1\leqslant s\leqslant\eta-1$ 的整数, 我们将 $C_k(Q)$ 分成 $2^s$ 个部分, 每个有长度 $R_s=Q2^{-s}$:

$$C_k(Q)=\sum_{g=1}^{2^s}\sum_{(g-1)R_s<x<gR_s}\mathrm{e}^{2\pi\mathrm{i}f(x)}$$
$$=\sum_{g=1}^{2^s}Z_{sg}\,(\text{定义}).$$

命 $Z=\{C_k(Q)\}^b$, 则

$$Z=\sum^{2^{sb}}Z_{sg_1}\cdots Z_{sg_b}, \tag{31}$$

此处 $\sum\limits^{M}$ 表示一个项数不超过 $M$ 的和 (在本文中, 我们恒用这一记号). 我们还用缩写记号

$$Z_s=Z_{s;g_1,\cdots,g_b}=Z_{sg_1}\cdots Z_{sg_b}.$$

具有佳位 $g_1,\cdots,g_b$ 的那些 $Z_{s;g_1,\cdots,g_b}$ 称为佳位和, 并记为 $Z_s'$. 由引理 3 可知非佳位和的个数不超过 $b!3^b2^{s(k-1)}$. 那些非佳位和 $Z_s$ 再继续分解, 即将每个因子分为两部分. 从而由每个非佳位和 $Z_s$, 我们得到 $2^b$ 个形如 $Z_{s+1}$ 的和 $Z_s$. 由所有非佳位和 $Z_s$ 得到的佳位和 $Z_{s+1}$ 的个数显然不超过

$$b!3^b2^{s(k-1)}\cdot 2^b=b!6^b2^{s(k-1)},$$

若这样获得的和 $Z_{s+1}$ 为佳位者, 则记为 $Z_{s+1}'$. 如上方法, 我们再分解其余的和. 由于 $Z_1$ 总是非佳位的, 所以我们总可以开始进行分解. 对于 $s=1,\cdots,\eta-1$, 重复这一步骤, 并用 $Z_\eta'$ 表示所有那些由非佳位的 $Z_{\eta-1}$ 获得的 $Z_\eta$, 于是得到

$$Z=\sum_{s=1}^{\eta}\sum^{M_s}Z_s', \tag{32}$$

此处 $M_s=b!6^62^{s(k-1)}$.

(ii) 由 Schwarg 不等式得

$$|C(Q)|^{2b}=|Z|^2\leqslant\eta\sum_{s=1}^{\eta}\left|\sum^{M_s}Z'_s\right|^2\leqslant\eta\sum_{s=1}^{\eta}M_s\sum^{M_s}|Z'_s|^2. \tag{33}$$

假定 $Z'_{s;g_1,\cdots,g_b}(1\leqslant s\leqslant\eta-1)$ 的 $g_1,\cdots,g_k$ 适合 (9); 否则我们可以重新安排指标. 由于几何平均不超过算术平均, 所以

$$|Z_{sg_{k+1}}\cdots Z_{sg_b}|^2\leqslant\frac{1}{b-k}\sum_{i=k+1}^{b}|Z_{sg_i}|^{2(b-k)}. \tag{34}$$

我们将 $Z_{sg_i}(k+1\leqslant i\leqslant b)$ 分成

$$\begin{aligned}[Q2^{-s}/(Q^{1-1/k}-1)]+1&\leqslant Q2^{-s}(Q^{1-1/k}-1)^{-1}+Q^{1/k}2^{-\eta}\\&\leqslant Q2^{-s}\left(\frac{3}{4}Q^{1-1/k}\right)^{-1}+Q^{1/k}2^{-s-1}\\&\leqslant Q^{1/k}2^{1-s}\end{aligned}$$

部分 (由于 $4\leqslant2^\eta\leqslant Q^{1/k}\leqslant Q^{1-\frac{1}{k}}$), 每一个具有形式

$$C^*=\sum_x \mathrm{e}^{2\pi\mathrm{i}f(x)},$$

此处 $x$ 过一个长度 $\leqslant Q^{1-\frac{1}{k}}-1$ 的区间, 即我们有一个整数 $\omega$ 满足

$$\omega<x\leqslant\omega+Q',\quad 0<Q'\leqslant Q^{1-1/k},\quad 0\leqslant\omega\leqslant g_iR_s\leqslant Q.$$

然后由 Hölder 不等式得

$$\begin{aligned}|Z_{sg_i}|^{2(b-k)}&\leqslant\left(\sum^{Q^{1/k}2^{1-s}}|C^*|\right)^{2(b-k)}\\&\leqslant(Q^{1/k}2^{1-s})^{2(b-k)-1}\sum^{Q^{1/k}2^{1-s}}|C^*|^{2(b-k)}.\end{aligned} \tag{35}$$

由 (33), (34) 与 (35) 得

$$|Z|^2\leqslant\frac{\eta}{b-k}\sum_{s=1}^{\eta}M_s(Q^{1/k}2^{1-s})^{2(b-k)-1}\sum^{N_s}|Z_{sg_1}|^2\cdots|Z_{sg_k}|^2|C^*|^{2(b-k)}, \tag{36}$$

此处 $N_s=M_s(b-k)Q^{1/k}2^{1-s}=b!6^b\cdot2^{s(k-1)}(b-k)Q^{1/k}2^{1-s}$. 在单位超立方体 $(0\leqslant\alpha_1\leqslant1,\cdots,0\leqslant\alpha_k\leqslant1)$ 上求积分得

$$\int_0^1\cdots\int_0^1|Z|^2\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k$$

$$\leqslant \frac{\eta}{b-k}\sum_{s=1}^{\eta} M_s(Q^{1/k}2^{1-s})^{2(b-k)-1}$$

$$\times \sum^{N_s} \int_0^1 \cdots \int_0^1 |Z_{sg_1}|^2 \cdots |Z_{sg_k}|^2 |C^*|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k. \tag{37}$$

(iii) 表达式

$$\int_0^1 \cdots \int_0^1 |Z_{sg_1}|^2 \cdots |Z_{sg_k}|^2 |C^*|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \tag{38}$$

等于丢番图方程组

$$x_1^h + \cdots + x_k^h + y_1^h + \cdots + y_{b-k}^h = x_1'^h + \cdots + x_k'^h + y_1'^h + \cdots + y_{b-k}'^h \quad (1 \leqslant h \leqslant k)$$

的解数, 此处诸 $y$ 位于形如

$$\omega < y, y' \leqslant \omega + Q' \quad (0 < Q' \leqslant Q^{1-1/k}; 0 \leqslant \omega \leqslant Q)$$

的一个区间中, 而 $x_i$ 与 $x_i'$ 位于诸区间

$$(g_i - 1)R_s < x_i, \quad x_i' \leqslant g_k R_s$$

之中, 其中当 $s \leqslant \eta - 1$ 时, 整数 $g_1, \cdots, g_k$ 满足条件 (9).

我们用 $X+\omega$ 代替 $x$ 及 $Y+\omega$ 代替 $y$, 则 (38) 亦等于方程组

$$X_1^h + \cdots + X_k^h + Y_1^h + \cdots + Y_{b-k}^h$$

$$= X_1'^h + \cdots + X_k'^h + Y_1'^h + \cdots + Y_{b-k}'^h \quad (1 \leqslant h \leqslant k) \tag{39}$$

的解数, 此处诸 $Y$ 位于区间 $(0, Q')$ 中, 而 $X_i$ 与 $X_i'$ 位于

$$-\omega + (g_i - 1)R_s < X_i, X_i' \leqslant -\omega + g_i R_s \quad (0 \leqslant \omega \leqslant Q) \tag{40}$$

之中.

现在, 若 $X'$ 任意固定, 则在 $X$ 上的条件适合引理 1 之要求, 其中 $R = R_s$, 及适合引理 2 之要求, 其中 $C = 2(b-k)$ 与 $H = 2^s$. 所以 $X$ 与 $X'$ 之集合个数不超过

$$R_s^k \{4(b-k)\}^k (2k2^s)^{\frac{1}{2}k(k-1)} Q^{\frac{1}{2}(k-1)}$$

$$= \{4(b-k)\}^k (2k)^{\frac{1}{2}k(k-1)} 2^{\frac{1}{2}sk(k-1)-sk} Q^{2k-\frac{1}{2}(k+1)}. \tag{41}$$

进而言之, 由于

$$\left|\int_0^1 f(x)\mathrm{e}^{\mathrm{i}xy}\mathrm{d}x\right| \leqslant \int_0^1 |f(x)|\mathrm{d}x,$$

所以对于固定的 $X$ 与 $X'$ 的集合, $Y$ 与 $Y'$ 的集合个数不超过

$$\int_0^1 \cdots \int_0^1 |C_k(Q^{1-1/k})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.$$

因此当 $1\leqslant s\leqslant \eta-1$ 时, 有

$$\begin{aligned}&\int_0^1 \cdots \int_0^1 |Z_{sg_1}\cdots Z_{sg_k}|^2|C^*|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ \leqslant&\{4(b-k)\}^k(2k)^{\frac12 k(k-1)}2^{\frac12 sk(k+1)-2sk}Q^{2k-\frac12(k+1)}\\ &\times\int_0^1 \cdots \int_0^1 |C_k(Q^{1-1/k})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.\end{aligned} \tag{42}$$

当 $s=\eta$ 时, 我们用寻常的不等式得

$$\begin{aligned}&\int_0^1 \cdots \int_0^1 |Z_{sg_1}\cdots Z_{sg_k}|^2|C^*|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ \leqslant&R_\eta^{2K}\int_0^1 \int_0^1 |C_k(Q^{1-1/k})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.\end{aligned} \tag{43}$$

由于

$$\begin{aligned}R_\eta^{2k}&=Q^{2k}2^{-2k\eta}\\ &\leqslant 2^{-\eta[2k-\frac12 k(k+1)]}Q^{2k-\frac12(k+1)}(Q2^{-\eta k})^{\frac12(k+1)}\\ &\leqslant 2^{-\eta[2k-\frac12 k(k+1)]}Q^{2k-\frac12(k+1)}2^{\frac12 k(k+1)}①,\end{aligned}$$

所以当 $s=\eta$ 时, (42) 亦成立.

(iv) 对于 $s=1,\cdots,\eta$ 时, 联合 (37) 与 (42) 得

$$\begin{aligned}&\int_0^1 \cdots \int_0^1 |C(Q)|^{2b}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ \leqslant&\eta\sum_{s=1}^{\eta} M_s(Q^{1/k}2^{1-s})^{2(b-k)-1}N_s\{4(b-k)\}^k\\ &\times(2k)^{\frac12 k(k-1)}2^{\frac12 sk(k+1)-2sk}Q^{2k-\frac12(k+1)},\\ &\int_0^1 \cdots \int_0^1 |C_k(Q^{1-1/k})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\end{aligned}$$

① 由于 $\eta\geqslant \log Q/k\log 2-1, \log 2^\eta\geqslant \log Q^{1/k}-\log 2=\log\frac12 Q^{1/k}$, 所以 $Q2^{-\eta k}\leqslant 2^k$.

$$
\begin{aligned}
&\leqslant \eta c \sum_{s=1}^{\eta} 2^{-s\{2b-\frac{1}{2}k(k+1)-2k\}} Q^{2k-\frac{1}{2}(k+1)+2(b-k)/k} \\
&\quad \times \int_0^1 \cdots \int_0^1 |C_k(Q^{1-1/k})|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \\
&\leqslant \eta^2 c Q^{2k-\frac{1}{2}(k+1)+2(b-k)/k} \int_0^1 \cdots \int_0^1 |C_k(Q^{1-1/k})|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k. \qquad (44)
\end{aligned}
$$

在此用到 $2b \geqslant \frac{1}{2}k(k+1) + 2k$, 其中

$$
c = (b!6^b)^2 2^{2(b-k)} (4b)^k (2k)^{\frac{1}{2}k(k-1)}.
$$

由于

$$
c < (12b)^{2b}(4b)^b(2k)^b \leqslant \{(12b)^2.4b.2b\}^b \leqslant (7b)^{4b},
$$

所以当 $\eta \geqslant 2$ 时, 定理成立.

(v) 情形 $\eta < 2$, 这时

$$
\frac{1}{k}\log Q/\log 2 < 2, \quad \text{即 } Q < 4^k.
$$

我们将 $C_k(Q)$ 分成四部分, 每一个皆具有形式

$$
C^* = \sum_{\omega < x \leqslant \omega + Q'} \mathrm{e}^{2\pi \mathrm{i} f(x)} \quad \left(0 < Q' \leqslant \frac{1}{4}Q \leqslant Q^{1-1/k}\right).
$$

由 Hölder 不等式可知

$$
|C_k(Q)|^{2b} \leqslant 4^{2b-1} \sum^4 |C^*|^{2b} \leqslant 4^{2b-1} Q^{2k(1-1/k)} \sum^4 |C^*|^{2(b-k)}.
$$

在单位超立方体上积分. 由于 $2b > \frac{1}{2}k(k+1)$, 所以

$$
\begin{aligned}
&\int_0^1 \cdots \int_0^1 |C_k(Q)|^{2b} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \\
&\leqslant 4^{2b-1} Q^{2k(1-1/k)} \sum^4 \int_0^1 \cdots \int_0^1 |C^*|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \\
&\leqslant 4^{2b} Q^{2k(1-1/k)} \int_0^1 \cdots \int_0^1 |C_k(Q^{1-1/k})|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \\
&\leqslant 4^{2b} Q^{2b-\frac{1}{2}(k+1)+2(b-k)/k} \int_0^1 \cdots \int_0^1 |C_k(Q^{1-1/k})|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k,
\end{aligned}
$$

定理证完.

## 4. 定理 1 的证明

若 $P^{1-1/k} \leqslant 3$, 则 $P \leqslant 9$, 从而定理显然成立. 所以我们假定 $P^{1-1/k} > 3$, 从而 $P > \mathrm{e}$.

当 $l = 0$ 时, 定理显然成立. 我们关于 $l$ 用归纳法. 假定定理对于 $l-1$ 真实, 则由定理 2 可知

$$\begin{aligned}&\int_0^1 \cdots \int_0^1 |C_k(P)|^{2s}\mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \\ \leqslant &(7s)^{4s} P^{2k-\frac{1}{2}(k+1)+2(s-k)/k} \\ &\times (\log P)^2 \int_0^1 \cdots \int_0^1 |C_k(P^{1-1/k})|^{2(s-k)}\mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k.\end{aligned} \tag{45}$$

由归纳法假定, 在定理 1 的陈述中以 $l-1, s-k$ 与 $P^{1-1/k}$ 代替 $l, s$ 与 $P$, 则当 $P^{1-1/k} > 3 > 2$ 时, 得

$$\begin{aligned}&\int_0^1 \cdots \int_0^1 |C_k(P^{1-1/k})|^{2(s-k)}\mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \\ \leqslant &(7s)^{4s(l-1)}(\log P)^{2(l-1)}P^{(1-1/k)\{2s-2k-\frac{1}{2}k(k+1)+\frac{1}{2}k(k+1)(1-1/k)^{l-1}\}}.\end{aligned} \tag{46}$$

联合 (45) 与 (46) 即得定理.

作为定理 1 的推论, 我们有

**定理 3**　命 $P \geqslant 2$ 及 $S \geqslant \frac{1}{4}k(k+1)+lk$. 则

$$\int_0^1 \left|\sum_{x=1}^{P} \mathrm{e}^{2\pi\mathrm{i}\alpha x^k}\right|^{2s} \mathrm{d}\alpha_1 \leqslant s^k (7s)^{4sl} (\log P)^{2l} P^{2k-k+\delta},$$

此处 $\delta = \frac{1}{2}k(k+1)\left(1-\frac{1}{k}\right)^l$.

**证明**　命 $r(N_1, \cdots, N_k)$ 为

$$x_1^h + \cdots + x_s^h - y_1^h - \cdots - y_s^h = N_h \quad (1 \leqslant h \leqslant k; 1 \leqslant x, y \leqslant P)$$

的解数. 则显然有

$$\int_0^1 \left|\sum_{x=1}^{P} \mathrm{e}^{2\pi\mathrm{i}\alpha x^k}\right|^{2s} \mathrm{d}\alpha_1 \leqslant \sum_{|N_1| \leqslant sP} \cdots \sum_{|N_{k-1}| \leqslant sP^{k-1}} r(N_1, \cdots, N_{k-1}, 0),$$

由于

$$r(N_1, \cdots, N_{k-1}, N_k)$$

$$= \int_0^1 \cdots \int_0^1 |C_k(P)|^{2s} e^{2\pi i(N_1\alpha_1+\cdots+N_k\alpha_k)} d\alpha_1 \cdots d\alpha_k$$
$$= \int_0^1 \cdots \int_0^1 |C_k(P)|^{2k} d\alpha_1 \cdots d\alpha_k.$$

故由定理 1 即得定理.

## 5. 指数和的估计

**引理 4** 命

$$\left|\alpha - \frac{h}{q}\right| \leqslant \frac{1}{q^2}, \quad (h,q)=1,$$

则

$$\sum_{y=1}^{Y}\left|\sum_{n=f+1}^{f+N} e^{2\pi i\alpha y n}\right| \leqslant \left(\frac{Y}{q}+1\right)(N+q\log q).$$

这一引理是熟知的; 关于其证明, 例如, 可见文献 [2].

**定理 4** 假定丢番图方程组

$$x_1^h + \cdots + x_{2t}^h = y_1^h + \cdots + y_{2t}^h \quad (1 \leqslant h \leqslant k; 1 \leqslant x,y \leqslant Q) \tag{47}$$

的解数不超过

$$c_1(k,t)P^{4l-\frac{1}{2}k(k+1)+\delta'}. \tag{48}$$

命 $F(x) = \alpha_{k+1}x^{k+1} + \cdots + \alpha_1 x + \alpha_0$,

$$S = \sum_{x=1}^{P} e^{2\pi i F(x)}$$

及

$$|\alpha_{k+1} - h/q| \leqslant q^{-2}, \quad (h,q)=1, \quad P \leqslant q \leqslant P^k. \tag{49}$$

则

$$|S| \leqslant c_2(k,t)P^{1-p}, \quad \rho = (1-\delta)/(4t+k-\delta). \tag{50}$$

**证明** 命 $p_1$ 为适合 $1 \leqslant p_1 \leqslant P$ 的一个整数及

$$S(y) = \sum_{x=1}^{P_1} e^{2\pi i F(x+y)},$$

则

$$S=\frac{1}{P_1}\sum_{x=1}^{p_1}\sum_{z=1}^{P}\mathrm{e}^{2\pi\mathrm{i}F(z)}=\frac{1}{p_1}\sum_{x=1}^{p_1}\sum_{y=1-x}^{P-x}\mathrm{e}^{2\pi\mathrm{i}F(x+y)}$$
$$=\frac{1}{p_1}\sum_{y=1}^{p}S(y)+Q_1p_1,\quad |Q_1|\leqslant 1. \tag{51}$$

记

$$F(x+y)=A_{k+1}x^{k+1}+A_kx^k+\cdots+A_0.$$

则

$$A_{k+1}=\alpha_{k+1},\quad A_k=\alpha_k+(k+1)\alpha_{k+1}y,\cdots \tag{52}$$

由 Hölder 不等式可知

$$\left|\sum_{y=1}^{p}S(y)\right|^{2t}\leqslant P^{2t-1}\sum_{y=1}^{p}|S(y)|^{2t}$$
$$=P^{2t-1}\sum_{y=1}^{P}\{S(y)\}^t\overline{\{S(y)\}^t}$$
$$=P^{2t-1}\sum_{y=1}^{p}\left(\sum_{x_1=1}^{P_1}\cdots\sum_{x_t=1}^{P_1}\sum_{x_1'=1}^{P_1}\cdots\sum_{x_t'=1}^{P_1}\mathrm{e}^{2\pi\mathrm{i}\phi}\right), \tag{53}$$

此处

$$\phi=f(x_1+y)+\cdots+f(x_t+y)-f(x_1'+y)-\cdots-f(x't+y)$$
$$=A_{k+1}\left(\sum_{i=1}^{t}x_i^{k+1}-\sum_{i=1}^{t}x_i'^{k+1}\right)+A_k\left(\sum_{i=1}^{t}x_i^k-\sum_{i=1}^{t}x_i'^k\right)+\cdots.$$

命 $\Psi(N_k,\cdots,N_1)$ 表示

$$x_1^h+\cdots+x_t^h-x_1'^h-\cdots-x_t'^h=N_h\quad(1\leqslant h\leqslant k;1\leqslant x,x'\leqslant p_1)$$

的解数. 则由 Schwarz 不等式可知

$$\sum_{y=1}^{p}|S(y)|^{2t}$$
$$\leqslant\sum_{x_1=1}^{p_1}\cdots\sum_{x_t=1}^{p_1}\sum_{x_1'=1}^{P_1}\cdots\sum_{x_t'=1}^{P_1}\left|\sum_{y=1}^{P}\mathrm{e}^{2\pi\mathrm{i}\phi}\right|$$
$$\leqslant\sum_{|N_1|\leqslant tp_1}\cdots\sum_{|N_k|\leqslant tp_1^k}\Psi(N_k,\cdots,N_1)\left|\sum_{y}\exp(A_kN_k+\cdots+A_1N_1)\right|$$

$$\leqslant \sqrt{\left\{\sum_{N_1}\cdots\sum_{N_k}\Psi^2(N_k,\cdots,N_1)\sum_{N_1}\cdots\sum_{N_k}\left|\sum_{y}\exp(A_kN_k+\cdots+A_1N_1)\right|^2\right\}}. \quad (54)$$

首先, 由 Parseval 关系式得表达式

$$\sum_{N_1}\cdots\sum_{N_k}\Psi^2(N_k,\cdots,N_1)=\sum_{N_1}\cdots\sum_{N_k}\left|\int_0^1\cdots\int_0^1\left|\sum_{x=1}^{p_1}\exp(\alpha_kx^k+\cdots+\alpha_1x)\right|^{2t}\right.$$
$$\left.\times\exp(-N_k\alpha_k-\cdots-N_1\alpha_1)\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\right|^2$$
$$=\int_0^1\cdots\int_0^1\left|\sum_{x=1}^{p_1}\exp(\alpha_kx^k+\cdots+\alpha_1x)\right|^{4t}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k,$$

所以由 (48) 得

$$\sum_{N_1}\cdots\sum_{N_k}r^2(N_1,\cdots,N_k)\leqslant c_1(k,t)p_1^{4t-\frac{1}{2}k(k+1)+\delta'}. \quad (55)$$

其次, 由 (52) 与引理 4, 得

$$\sum_{|N_1|\leqslant tp_1}\cdots\sum_{|N_k|\leqslant tp_1^k}\left|\sum_{y}\mathrm{e}^{2\pi\mathrm{i}(A_kN_k+\cdots+A_1N_1)}\right|^2$$
$$\leqslant t^kp_1^{1+\cdots+k-1}\sum_{y_1=1}^{P}\sum_{y_2=1}^{P}\left|\sum_{N_k}\mathrm{e}^{2\pi\mathrm{i}(k+1)\alpha_{k+1}(y_1-y_2)N_k}\right|$$
$$\leqslant t^kp_1^{\frac{1}{2}k(k-1)}P\sum_{Y=1}^{P}\left|\sum_{N_k}\mathrm{e}^{2\pi\mathrm{i}\alpha_{k+1}YN_k}\right|$$

(由于 $(k+1)(y_1-y_2)=Y$ 的解数不超过 $P$)

$$\leqslant c_3(k,t)p_1^{\frac{1}{2}k(k-1)}P\left(\frac{P}{q}+1\right)(p_1^k+q\log q). \quad (56)$$

联合 (54), (55), (56) 得

$$\sum_{y}|S(y)|^{2t}\leqslant c_4(k,t)p_1^{2t+\frac{1}{2}\delta}P^{\frac{1}{2}}(1+p_1^{-k}q\log q)^{\frac{1}{2}}.$$

从而由 (53) 得

$$|S|\leqslant c_5(k,t)p_1^{\delta/4t}P^{1-1/4t}(1+p_1^{-k}q\log q)^{1/4t}+p_1.$$

对于 $P\leqslant q\leqslant P^k$, 我们有

$$|S|\leqslant c_5(k,t)(p_1^{(\delta-k)/4t}P^{1+(k-1)/4t}+p_1)\log P.$$

取

$$p_1 = P^{1-\rho}, \quad \rho = \frac{1-\delta}{4t+k-\delta},$$

定理证完.

**定理 5**　命 $k > 10$, 及

$$\left|\alpha - \frac{h}{q}\right| \leqslant \frac{1}{q^2}, \quad (h,q)=1, \quad P \leqslant q \leqslant P^{k-1},$$

则

$$\left|\sum_{x=1}^{P} \mathrm{e}^{2\pi \mathrm{i}\alpha x^k}\right| \leqslant c_6(k) P^{1-1/\sigma}, \quad \sigma = 4k^2\left(\log k + \frac{1}{2}\log\log k + 3\right).$$

**证明**　取

$$t = \left[\frac{1}{8}k(k-1) + \frac{l(k-1)}{2}\right] + 1,$$

$$l = \left[\frac{\log\left\{\frac{1}{2}k(k-1)\right\} + \log\log k}{-\log\{1-1/(k-1)\}}\right] + 1,$$

则得

$$\delta = \frac{1}{2}k(k-1)\left(1-\frac{1}{k-1}\right)^l < 1/\log k \quad \left(<\frac{1}{2}\right).$$

由定理 1 可知定理 4 的假定成立, 其中 $\delta' = 1/\log k$.

由于

$$-1/\log\left(1-\frac{1}{k-1}\right) \leqslant k,$$

$$\begin{aligned} 2l + \frac{1}{2}k &\leqslant 2k\left(\log\frac{1}{2}h^2 + \log\log k\right) + \frac{1}{2}k + 1 \\ &< 2k(\log k^2 + \log\log k), \end{aligned}$$

所以

$$\begin{aligned} \frac{4t-k-1-\delta}{1-\delta} &\leqslant \frac{\left(2l+\frac{1}{2}k\right)(k-1)-k+3-\delta}{1-\delta} \\ &< \left(2l+\frac{1}{2}k\right)k(1+2\delta) \\ &\leqslant 4k^2\left(\log k + \frac{1}{2}\log\log k + 2 + \log\log k/\log k\right) \\ &\leqslant 4k^2\left(\log k + \frac{1}{2}\log\log k + 3\right). \end{aligned} \tag{57}$$

由于 (57) 是一个开号不等式, 所以由定理 4 即得定得.

## 6. 应　　用

在本节中, 我们仅仅指出若干应用. 这些只要对熟知的方法作一点简单的改动即能得到.

(i) Waring-Goldbach 问题. 命 $H(k)$ 为使

$$P_1^k + \cdots + P_s^k = N \tag{58}$$

对于充分大的 $N$ 可解的最小整数 $s$, 在此需假定 $N$ 满足某些同余条件, 用作者文 [3] 的方法之一并用定理 5 的新指数代替旧的指数, 即得

$$H(k) \leqslant s_0 \quad (\sim 4k\log k, k\text{充分大}).$$

(ii) 当 $s \geqslant s_0 = 4k^2\left(\log k + \frac{1}{2}\log\log k + 8\right)$ 时, (58) 的解数的渐近公式成立. 实际上, 当 $s$ 适合这一界时, 我们也可以证明将一个整数分拆成 $s$ 个正 $k$ 次方幂的分拆个数的 Hardy-Littewood 渐近公式成立. 这比 Viwogradov[4] 的界 $s \geqslant s_0 = 10k^2\log k$ 要精密一些.

### 参 考 文 献


[1] Vinogradov 方法的最新版本. 见 Bull. de l'Acad. *des Sci. de L'URSS*, 1942, 6: 33–40.

[2] Landau. *Vorlesungen Über Zahlentheovie*, Bd. 1: 256.

[3] 华罗庚. *Math. Zeits*, 1939, 44: 335–346.

[4] Vinogradov. Comptes Rendus (Doklaly).


**1949 年 7 月 20 日注记**　我感谢 J.L.B.Cooper 博士告诉我; 我的书已于 1947 年作为 Stekloff 数学研究所的专著第 22 号出版了. 他亦给我看了 Vinogradov 的专著, 在其中包含了 (ii)§6 的结果的证明, 其中 $s \geqslant 10k^2\log k$, 似乎值得一提的是定理 5 的指数比他的结果略为好一点. 他是用

$$\sigma = 3k^2\log\{12(k+1)k\} \quad (\sim 6k^2\log k)$$

代替了本文之

$$\sigma = 4k^2\left(\log k + \frac{1}{2}\log\log k + 3\right).$$

(潘承彪　译)

# 代数数域上的指数和[①]

华罗庚 (北京, 国立清华大学)

## 1. 导　　言

命 $K$ 为一个关于有理数域的 $n$ 次代数数域, 及 $\mathfrak{d}$ 为域的基理想 (分歧), 命

$$f(x) = \alpha_k x^k + \cdots + \alpha_1 x + \alpha_0$$

为一个系数属于 $K$ 的 $k$ 次多项式, 及 $\mathfrak{a}$ 为由 $\alpha_k, \cdots, \alpha_1$ 生成的分数理想, 即 $\mathfrak{a} = (\alpha_k, \cdots, \alpha_1)$. 假定 $\mathfrak{a}\mathfrak{d} = \mathfrak{r}/\mathfrak{q}$, 此处 $\mathfrak{r}$ 与 $\mathfrak{q}$ 为互素的两个整理想, 及

$$S(f(x), \mathfrak{q}) = S(f(x)) = S(\mathfrak{q}) = \sum_{x \bmod \mathfrak{q}} \mathrm{e}^{2\pi i tr(f(x))},$$

此处 $x$ 过 $\bmod \mathfrak{q}$ 的一个完全剩余系, 本文的目的为证明下面的定理.

**定理 1**　对于任何 $\varepsilon > 0$, 我们有

$$S(f(x), \mathfrak{q}) = O(N(\mathfrak{q})^{1-1/k+\varepsilon}),$$

此处与记号 $O$ 有关的常数仅依赖于 $k, n$ 及 $\varepsilon$.

如同通常一样, 我们用 $\mathrm{tr}(\alpha)$ 与 $N(\mathfrak{q})$ 分别表示 $K$ 中的数 $\alpha$ 的迹及理想 $\mathfrak{q}$ 的范数.

这是作者[1] 关于有理数域上一条定理的推广. 但在此所用的方法与原来的方法相比有较大差异与简化.

## 2. 关于同余式的一条定理

**定理 2**　命 $\mathfrak{p}$ 为一个素理想及 $s(x)$ 为一个整系数 $\bmod \mathfrak{p}$ 的多项式, 命 $\alpha$ 为同余式

$$s(x) \equiv 0 (\bmod \mathfrak{p})$$

的 $m$ 重根, 命 $\lambda$ 为一个整数, 它可以被 $\mathfrak{p}$ 整除, 但不能被 $\mathfrak{p}^2$ 整除, 又命 $u$ 为最大的整数使 $\mathfrak{p}^u$ 能整除 $s(\lambda x + \alpha) - s(\alpha)$ 的所有系数及

---

① 1949 年 9 月 14 日收到. 发表于 *Canadian J. Math.*, 1951, 3: 44–51.

$$t(x) \equiv \lambda^{-u}(s(\lambda x+\alpha)-s(\alpha))(\operatorname{mod}\mathfrak{p})$$

为一个整系数多项式, 则 $u \leqslant m$, 及同余式

$$t(x) \equiv 0(\operatorname{mod}\mathfrak{p})$$

最多只有 $m$ 个解.

**证明** 不失一般性, 我们可以假定 $\alpha=0$, 则

$$s(x) \equiv x^m s_1(x)+s_2(x), \quad s_1(0) \not\equiv 0(\operatorname{mod}\mathfrak{p}),$$

此处 $s_2(x)$ 为一个次数小于 $m$ 的多项式, 它的所有系数皆可以被 $\mathfrak{p}$ 整除. 我们有

$$s(\lambda x) \equiv \lambda^m x^m s_1(\lambda x)+s_2(\lambda x).$$

由于 $x^m$ 的系数为 $\lambda^m s_1(0)$, 它不能被 $\mathfrak{p}^{m+1}$ 整除, 所以 $u \leqslant m$.

由于 $\lambda^{-u}s(\lambda x)$ 同余于一个次数不超过 $m$ 的多项式, $\operatorname{mod}\mathfrak{p}$, 故得定理.

**附记** $u$ 与 $\lambda$ 的选取是独立的, 事实上, 命 $\lambda'$ 为另一个有同样性质的整数, 则有一个整数 $\tau$ 满足

$$\lambda \equiv \lambda'\tau(\operatorname{mod} p^{u+1}), \quad \mathfrak{p} \nmid \tau.$$

$$s(\lambda x+a)-s(\alpha) \equiv s(\lambda'(\tau x)+a)-s(a)\ (\operatorname{mod}\mathfrak{p}^{u+1}).$$

## 3. 关于代数数的几条引理

命 $\mathfrak{g}$ 为一个分数或整数理想及 $\mathfrak{a}$ 为一个整理想, 则显然有 $\mathfrak{g}|\mathfrak{g}\mathfrak{a}$.

现在我们按照模 $\mathfrak{g}\mathfrak{a}$ 将 $\mathfrak{g}$ 的元素分成剩余类, 则不同的类的个数为 $N(\mathfrak{a})$. 在每一类中取一个元素, 则这样组成的集合称为 $\mathfrak{g}$ 的一个完全剩余系 $\operatorname{mod}\mathfrak{g}\mathfrak{a}$.

基理想 $\mathfrak{d}$ 的定义可以用下面的方法来陈述.

$\mathfrak{d}^{-1}$ 为 $K$ 中所有满足

$$\mathrm{e}^{2\pi\mathrm{i}\operatorname{tr}(\xi\alpha)}=1$$

的数 $\xi$ 的集合, 其中 $\alpha$ 过 $K$ 中所有整数. 从而若 $\beta$ 属于 $(\mathfrak{q}\mathfrak{d})^{-1}$ 及 $\alpha_1 \equiv \alpha_2(\operatorname{mod}\mathfrak{q})$, 则

$$\mathrm{e}^{2\pi\mathrm{i}\operatorname{tr}(\beta\alpha_1)}=\mathrm{e}^{2\pi\mathrm{i}\operatorname{tr}(\beta\alpha_2)}.$$

这说明本文开始定义的和 $S(f(x),\mathfrak{q})$ 是独立于 $\operatorname{mod}\mathfrak{q}$ 的剩余类的选取的.

**定理 3** 命 $\mathfrak{q}$ 为一个整理想, 当 $\xi$ 过 $(\mathfrak{q}\mathfrak{d})^{-1}$ 的一个完全剩余系 $\operatorname{mod}\mathfrak{d}^{-1}$ 时, 对于每一个整数 $\alpha$, 我们皆有

$$\sum_{\xi}\mathrm{e}^{2\pi\mathrm{i}\operatorname{tr}(\xi\alpha)}=\begin{cases} N(\mathfrak{q}), & 当\ \mathfrak{q}|\alpha, \\ 0, & 当\ \mathfrak{q}\nmid\alpha. \end{cases}$$

**证明** 若 $\mathfrak{q}|\alpha$, 则 $\xi\alpha \in \mathfrak{d}^{-1}$, 所以对于所有 $\xi$, 我们皆有 $e^{2\pi i \mathrm{tr}(\xi\alpha)} = 1$, 故得第一个结论.

若 $\mathfrak{q} \nmid \alpha$, 则存在一个 $(\mathfrak{d}\mathfrak{q})^{-1}$ 的元素 $\xi_0$. 但 $\xi_0\alpha$ 不属于 $\mathfrak{d}^{-1}$. 事实上, 若对所有属于 $(\mathfrak{d}\mathfrak{q})^{-1}$ 的 $\xi_0$, 皆有 $\xi_0\alpha$ 属于 $\mathfrak{d}^{-1}$, 则有

$$\mathfrak{d}^{-1}|\alpha(\mathfrak{d}\mathfrak{q})^{-1},$$

因此得 $\mathfrak{q}|\alpha$. 这是不可能的, 所以由 $\mathfrak{d}^{-1}$ 的定义可知, 存在一个整数 $\gamma$ 满足

$$e^{2\pi i \mathrm{tr}(\gamma\xi_0\alpha)} \neq 1.$$

由于 $\gamma\xi_0 \in (\mathfrak{d}\mathfrak{q})^{-1}$, 我们可以记 $\gamma\xi_0 = \xi_1$. 所以

$$\sum_{\xi} e^{2\pi i \mathrm{tr}(\xi\alpha)} = \sum_{\xi} e^{2\pi i \mathrm{tr}((\xi+\xi_1)\alpha)} = e^{2\pi i \mathrm{tr}(\xi_1\alpha)} \cdot \sum_{\xi} e^{2\pi i \mathrm{tr}(\xi\alpha)}.$$

故得定理的第二个结论.

## 4. 对于 $\mathfrak{q} = \mathfrak{p}$ 时的定理证明

当 $\mathfrak{q}$ 为一个素理想 $\mathfrak{p}$ 时, 这里所考虑的指数和归结为有限域上的一种指数和, 在以前的文章[2] 已有讨论. 但作者还不能找到一个简单的途径来建立这里所考虑的指数和与那里讨论的有限域上的指数和之间的显式关系. 为了完整起见, 在此仍给了一个证明, 其中所用的方法是属于 Morderll[3] 的.

**定理 4** 我们有

$$|S(f(x), \mathfrak{p})| \leqslant k^n N(\mathfrak{p})^{1-1/k}.$$

**证明** 不失一般性, 我们可以假定 $\alpha_k$ 不属于 $\mathfrak{d}^{-1}$, 否则, 由于对于所有整数 $x$ 皆有 $e^{2\pi i \mathrm{tr}(\alpha_k x^k)} = 1$, 所以

$$S(f(x), \mathfrak{p}) = S(f(x) - \alpha_k x^k, \mathfrak{p}),$$

因此我们现在假定 $\alpha_k$ 属于 $(\mathfrak{p}\mathfrak{d})^{-1}$, 但不属于 $\mathfrak{d}^{-1}$, 由于当 $N(\mathfrak{p}) \leqslant k^n$ 时,

$$|S(f(x), \mathfrak{p})| \leqslant N(\mathfrak{p}) \leqslant k^n N(\mathfrak{p})^{1-1/k}.$$

即定理成立.

现在我们假定 $N(\mathfrak{p}) > k^n$, 从而 $\mathfrak{p} \nmid k!$. 我们有

$$|S(f(x))|^{2k} = \frac{1}{N(\mathfrak{p})(N(\mathfrak{p})-1)} \sideset{}{'}\sum_{\lambda \bmod \mathfrak{p}} \sum_{\mu \bmod \mathfrak{p}} |S(f(\lambda x + \mu))|^{2k},$$

此处 $\lambda$ 过 $\bmod \mathfrak{p}$ 的一个缩剩余系. 记

$$f(\lambda x+\mu)=\beta_k x^k+\cdots+\beta_0,$$

此处

$$\beta_k \equiv a_k \lambda^k (\bmod \mathfrak{d}^{-1}), \tag{1}$$

$$\beta_{k-1} \equiv k a_k \lambda^{k-1}+a_{k-1}\lambda^{k-1} (\bmod \mathfrak{d}^{-1}), \tag{2}$$

等等.

对于属于 $(\mathfrak{p}\mathfrak{d})^{-1}$ 固定的 $\beta_k, \beta_{k-1}, \cdots$, 整数 $\lambda$ 与 $\mu$ 的个数不超过 $k$. 事实上, (1) 表明 $\beta_k-\alpha_k\lambda^k$ 属于 $\mathfrak{d}^{-1}$ ($\beta_k$ 与 $\alpha_k$ 属于 $(\mathfrak{p}\mathfrak{d})^{-1}$). 存在一个整数属于 $\mathfrak{p}\mathfrak{d}$ 但不属于 $\mathfrak{p}$. 从而 $\tau\alpha_k$ 与 $\tau\beta_k$ 都是整数及 $\mathfrak{p}\nmid\tau\alpha_k$; 显然同余式 $\tau\beta_k\equiv\tau\alpha_k\lambda^k(\bmod \mathfrak{p})$ 最多只有 $k$ 个解. 对于固定的 $\lambda$, 由于 $\mathfrak{p}\nmid k$, 同理可知 $\mu$ 由 (2) 唯一地确定.

因此

$$|S(f(x),\mathfrak{p})|^{2k} \leqslant \frac{k}{N(\mathfrak{p})(N(\mathfrak{p})-1)}\sum_{\beta_k}\cdots\sum_{\beta_1}|S(\beta_k x^k+\cdots+\beta_1 x)|^{2k},$$

此处每个 $\beta$ 皆过 $(\mathfrak{p}\mathfrak{d})^{-1}$ 的一个完全剩余系, $\bmod \mathfrak{d}^{-1}$.

我们有

$$\begin{aligned}&\sum_{\beta_k}\cdots\sum_{\beta_1}|S(\beta_k x^k+\cdots+\beta_1 x)|^{2k}\\=&\sum_{\beta_k}\cdots\sum_{\beta_1}\sum_{x_1}\cdots\sum_{x_k}\sum_{y_1}\cdots\sum_{y_k}\mathrm{e}^{2\pi i \mathrm{tr}(\Psi)}\\=&N(\mathfrak{p})^k M,\end{aligned}$$

此处

$$\begin{aligned}\psi=&\beta_k(x_1^k+\cdots+x_k^k-y_1^k-\cdots-y_k^k)\\&+\beta_{k-1}(x_1^{k-1}+\cdots+x_k^{k-1}-y_1^{k-1}-\cdots-y_k^{k-1})+\cdots\\&+\beta_1(x_1+\cdots+x_k-y_1-\cdots-y_k),\end{aligned}$$

及由定理 3 可知 $M$ 等于同余式组

$$x_1^h+\cdots+x_k^h\equiv y_1^h+\cdots+y_k^h, \bmod \mathfrak{p}, \quad 1\leqslant h\leqslant k$$

的解数.

由于 $\mathfrak{p}\nmid k!$, 所以由对称函数的一条定理得

$$(X-x_1)\cdots(X-x_k)\equiv(X-y_1)\cdots(X-y_k), \bmod \mathfrak{p},$$

因此我们得知 $x_1,\cdots,x_k$ 为 $y_1,\cdots,y_k$ 的一个置换, 及

$$M \leqslant k!N(\mathfrak{p})^k.$$

从而

$$\begin{aligned}|S(f(x),\mathfrak{p})|^{2k} &\leqslant \frac{k\cdot k!}{N(\mathfrak{p})(N(\mathfrak{p})-1)}N(\mathfrak{p})^{2k}\\ &\leqslant 2k\cdot k!N(\mathfrak{p})^{2k-2}\\ &\leqslant k^{2k}N(\mathfrak{p})^{2k-2},\end{aligned}$$

定理证完.

## 5. 对于 $\mathfrak{q}=\mathfrak{p}^l$ 时的定理证明

**定理 5** 若 $\mathfrak{q}=\mathfrak{p}^l$ 及 $\mathfrak{p}$ 为一个素理想, 则

$$|S(f(x),\mathfrak{p}^l)\leqslant k^{2n+1}N(\mathfrak{p}^l)^{1-1/k}. \tag{3}$$

**证明** 命

$$\mathfrak{b}=(k\alpha_k,(k-1)\alpha_{k-1},\cdots,2\alpha_2,\alpha_1).$$

显然 $\mathfrak{a}|\mathfrak{b}$. 命 $t$ 为整除 $\mathfrak{b}\mathfrak{a}^{-1}$ 的 $\mathfrak{p}$ 的最高幂次. 当 $x$ 过 $\bmod \mathfrak{p}$ 的一个完全剩余系时, 命 $m$ 表示同余式

$$f'(x)\equiv 0(\bmod \mathfrak{p}^{t+1-l}) \tag{4}$$

的解数, 其中解的重数计算在内 (我们有 $m\leqslant k-1$).

显然 (3) 是下面更强的结果的推论:

$$|S(f(x),\mathfrak{p}^l)|\leqslant k^{2n}\max(1,m)N(\mathfrak{p}^l)^{1-1/k}. \tag{5}$$

若 $t\geqslant 1$, 则 $\mathfrak{p}^t$ 至少能整除整数 $k,k-1,\cdots,1$ 中的一个. 所以

$$N(\mathfrak{p}^t)\leqslant k^n,$$

即

$$N(\mathfrak{p})\leqslant k^{n/t}. \tag{6}$$

假定 $l<2(t+1)$, 当 $t=0$ 时得 $l=1$ 及由定理 4 即得 (3). 若 $t\geqslant 1$, 则由 (6) 可知

$$\begin{aligned}|S(f(x),\mathfrak{p}^l)| &\leqslant N(\mathfrak{p})^l\leqslant (N(\mathfrak{p})^{l(1-1/k)}(N(\mathfrak{p}))^{(2t+1)/k}\\ &\leqslant N(\mathfrak{p})^{l(1-1/k)}k^{n(2+1/t)/k}\\ &\leqslant k^{2n}\cdot N(\mathfrak{p})^{l(1-1/k)}.\end{aligned}$$

所以当 $l\leqslant 2t+1$ 时, (5) 成立. 现在假定 $l\geqslant 2(t+1)$ 及 (5) 对于较小的 $l$ 成立.

命 $\mu_1,\cdots,\mu_r$ 为 (4) 的不同的根, 其重数分别为 $m_1,\cdots,m_r$, 则 $m_1+\cdots+m_r=m$. 显然有

$$S(f(x))=\sum_x \mathrm{e}^{2\pi i\mathrm{tr}(f(x))}=\sum_\nu \sum_{\substack{x\\ x\equiv\nu(\bmod \mathfrak{p})}} \mathrm{e}^{2\pi i\mathrm{tr}(f(x))}=\sum_\nu S_\nu(\text{定义}),$$

此处 $\nu$ 过 $\bmod \mathfrak{p}$ 的一个完全剩余系, 若 $\nu$ 不是诸 $\mu$ 中的一个, 则命

$$x=y+\lambda^{l-t-1}z,$$

此处 $\lambda$ 为 $\mathfrak{p}$ 中一个整数, 但 $\lambda$ 不属于 $\mathfrak{p}^2$. 由于 $\mathfrak{p}^{t+1-l}\nmid f'(y)$. 所以由定理 3 可知

$$\begin{aligned}S_\nu&=\sum_{\substack{y\bmod \mathfrak{p}^{l-t-1}\\ y\equiv\nu(\bmod \mathfrak{p})}}\sum_{z\bmod \mathfrak{p}^{t+1}} \mathrm{e}^{2\pi i\mathrm{tr}(f(y)+\lambda^{l-t-1}zf'(y))}\\&=\sum \mathrm{e}^{2\pi i\mathrm{tr}(f(y))}\sum_{z\bmod \mathfrak{p}^{t+1}} \mathrm{e}^{2\pi i\mathrm{tr}(\lambda^{l-t-1}zf'(y))}=0,\end{aligned}$$

所以

$$\begin{aligned}|S(f(x))|&\leqslant\sum_{s=1}^r\left|\sum_{x\bmod \mathfrak{p}^{l-1}} \mathrm{e}^{2\pi i\mathrm{tr}(f(\mu_s+\lambda y))}\right|\\&=\sum_{s=1}^r\left|\sum_{x\bmod \mathfrak{p}^{l-1}} \mathrm{e}^{2\pi i\mathrm{tr}(f(\mu_s+\lambda y)-f(\mu_s))}\right|\\&=\sum_{s=1}^r N(\mathfrak{p})^{\sigma_s-1}S(f(\mu_s+\lambda y)-f(\mu_s),\mathfrak{p}^{l-\sigma_s}),\end{aligned}\tag{7}$$

此处 $\sigma_s$ 是由下面方法来定义的: 命 $\mathfrak{c}$ 为由

$$f_s(y)=f(\mu_s+\lambda y)-f(\mu_s)$$

的系数生成的理想. 显然 $\mathfrak{a}$ 整除 $\mathfrak{c}$. 命 $\sigma_s$ 为能整除 $\mathfrak{c}\mathfrak{a}^{-1}$ 的 $\mathfrak{p}$ 的最高幂次. 同时, 若 $l\leqslant\sigma_s$, 则我们用习惯的方法:

$$S(f(\mu_s+\lambda y)-f(\mu_s),\mathfrak{p}^{l-\sigma_s})=\mathfrak{p}^{l-\sigma_s}.$$

今往证明

$$1\leqslant\sigma_s\leqslant k.\tag{8}$$

若 (8) 不真实, 则 $\mathfrak{p}^{-l+k+1}$ 能整除 $f(\mu_s+\lambda y)-f(\mu_s)$ 的所有系数, 即

$$\mathfrak{p}^{-l+k+1}\left|\frac{f^{(r)}(\mu_s)}{r!}\lambda^r,\quad 1\leqslant r\leqslant k.\right.$$

从而

$$\mathfrak{p}^{-l+1}\left|\frac{f^{(r)}(\mu_s)}{r!}\right.,$$

它等于 $\alpha_r$ 加上 $\alpha_k,\cdots,\alpha_{r-1}$ 的整系数的线性组合. 因此我们可以逐次推出 $\mathfrak{p}^{-l+1}\times|\alpha_k, \mathfrak{p}^{-l+1}|\alpha_{k-1},\cdots,\mathfrak{p}^{-l+1}|\alpha_1$, 这与 $\mathfrak{q}=\mathfrak{p}^l$ 相矛盾.

由 (7) 与 (8) 可知当 $l\geqslant\max(\sigma,\cdots,\sigma_r)$ 时,

$$|S(f(x),\mathfrak{p}^l)|\leqslant\sum_{s=1}^{r}N(\mathfrak{p})^{\sigma_s(1-1/k)}|S(f_s(y),\mathfrak{p}^{l-\sigma_s})|.$$

由归纳法假定可知

$$\begin{aligned}|S(f(x),\mathfrak{p}^l)|&\leqslant k^{2n}\sum_{s=1}^{r}N(\mathfrak{p})^{\sigma_s(1-1/k)}m_sN(\mathfrak{p})^{(l-\sigma_s)(1-1/k)}\\&=k^{2n}mN(\mathfrak{p})^{l(1-1/k)}.\end{aligned}$$

对于 $l\leqslant\max(\sigma_1,\cdots,\sigma_r)$, 我们有 $l\leqslant k$, 及由 (7) 得

$$|S(f(x))|\leqslant r\mathfrak{p}^{l-1}\leqslant m\mathfrak{p}^{l(1-1/k)}.$$

故得 (5), 从而得 (3) $\left(\text{注意, 若 }\sum_{s=1}^{r}m_s=0\text{, 则这一方法推出当 }l\geqslant 2(t+1)\text{ 时, }S(f(x))=0\right)$.

**定理 6**　若 $(\mathfrak{q}_1,\mathfrak{q}_2)=1$ 及 $f(0)=0$, 则存在 $k$ 次多项式 $f_1(x)$ 与 $f_2(x)$, 使

$$S(f(x),\mathfrak{q}_1\mathfrak{q}_2)=S(f_1(x),\mathfrak{q}_1)S(f_2(x),\mathfrak{q}_2).$$

**证明**　我们可以找到两个整数 $\lambda_1$ 与 $\lambda_2$ 使

$$(\lambda_1,\mathfrak{q}_1\mathfrak{q}_2)=\mathfrak{q}_2,\quad(\lambda_2,\mathfrak{q}_1\mathfrak{q}_2)=\mathfrak{q}_1.$$

置

$$x=\lambda_1y_2+\lambda_2y_1,$$

则当 $y_1$ 与 $y_2$ 分别过 $\bmod\mathfrak{q}_1$ 与 $\bmod\mathfrak{q}_2$ 的完全剩余系时, $x$ 过 $\bmod\mathfrak{q}_1\mathfrak{q}_2$ 的一个完全剩余系, 所以

$$\begin{aligned}S(f(x),\mathfrak{q}_1\mathfrak{q}_2)&=\sum_{y_1\bmod\mathfrak{q}_1}\sum_{y_2\bmod\mathfrak{q}_2}\mathrm{e}^{2\pi i\mathrm{tr}(f(\lambda_1y_2+\lambda_2y_1))}\\&=\sum_{y_1\bmod\mathfrak{q}_1}\mathrm{e}^{2\pi i\mathrm{tr}(f(\lambda_2y_1))}\sum_{y_2\bmod\mathfrak{q}_2}\mathrm{e}^{2\pi i\mathrm{tr}(f(\lambda_1y_2))}\\&=S(f_1(x),\mathfrak{q}_1))S(f_2(x),\mathfrak{q}_2),\end{aligned}$$

此处 $f_1(x)=f(\lambda_2x)$ 及 $f_2(x)=f(\lambda_1x)$, 现在我们来验证 $f_1(x)$ 的系数生成的理想可以表示为 $\mathfrak{r}(\mathfrak{d}\mathfrak{q}_1)^{-1}$, 此处 $\mathfrak{r},\mathfrak{q}$ 为互素的整理想, 这是显然的.

## 6. 定理 1 的证明

命

$$\mathfrak{q} = \mathfrak{p}_1^{l_1} \cdots \mathfrak{p}_s^{l_s},$$

则不断应用定理 6 可知

$$S(f(x), \mathfrak{q}) = \prod_{i=1}^{s} S(f_i(x), \mathfrak{p}_i^{l_i}).$$

由定理 5 得

$$\begin{aligned}|S(f(x), \mathfrak{q})| &\leqslant \sum_{i=1}^{s} k^{2n+1} N(\mathfrak{p}_i^{l_i})^{1-1/k} \\ &\leqslant \sum_{i=1}^{s} (1 + l_i)^{(2n+1)\log k/\log 2} N(\mathfrak{p}_i^{l_i})^{(1-1/k)} \\ &= d(\mathfrak{q})^{(2n+1)\log k/\log 2} N(\mathfrak{q})^{1-1/k} \\ &= O(N(\mathfrak{q})^{1-1/k+\varepsilon}),\end{aligned}$$

此处 $d(\mathfrak{q})$ 表示 $\mathfrak{q}$ 的因子个数.

**附记** 实际上, 上面的方法为一个算法; 更明确地, 对于已给一个多项式, 若我们知道 $S(f(x), \mathfrak{p}^l)$ 之值, 其中 $l \leqslant 2t + 1$, 则我们可以求出 $S(f(x), \mathfrak{p}^l)$ 之值.

### 参 考 文 献


[1] 华罗庚. On an exponential sum. *Jour. of Chinese Math. Soc.*, 1940, 2: 301–312.

[2] 华罗庚与闵嗣鹤. On a double exponential sum, *Acad. Sinica Sci. Record*, 1942, 1: 23–25.

[3] L. J. Mordell. On a sum analogous to a Gauss's sum. *Quart. J. Math.* (Oxford), 1932, 3: 161–167.


(潘承彪 译)

# 一个求极限的问题①

华罗庚 (清华大学, 中国科学院数学研究所)

命 $\omega(u)$ 是 $u$ 的实函数, 当 $u \geqslant 1$ 时, 其定义如下:

$$\begin{cases} \omega(u) = u^{-1}, & 1 \leqslant u \leqslant 2; \\ \dfrac{\mathrm{d}}{\mathrm{d}u}(u\omega(u)) = \omega(u-1), & u > 2. \end{cases} \tag{1}$$

在 1937 年苏联数学家Бухштаб[1] 求出

$$\lim_{u \to \infty} \omega(u) = e^{-\gamma}, \tag{2}$$

此处 $\gamma$ 是 Euler 常数. 这结果是他研究数论的副产物, 原来的证明是用数论上的 Brun 氏方法得出的! 显而易见, 这是一个纯解析的问题, 因为无论是 $\omega(u)$ 的定义也好, 结论也好, 都没有丝毫的数论味儿, 因此就发生了一个问题, 就是可否用解析的方法来证明这解析上的命题. 直到 1950 年, 荷兰数学家 De Bruijn 用解析方法才证明了这一命题, 但在 1951 年Бухштаб 用数论的方法更精密地证出了

$$|\omega(u) - \mathrm{e}^{-\gamma}| < \mathrm{e}^{-u(\log u + \log\log u - 1) + O(u \log\log u / \log u)}. \tag{3}$$

在这一篇文章中, 我将用解析方法来证明一个比 (3) 稍精密些的结果. 凡懂得高等微积分的读者, 就能了解我的证明. 为了使读者易于接受, 其中对某一方法写得较详尽些, 但对读者易于补出的地方 (例如: 积分号下求微分、变换极限与积分的次序等等), 则略去.

**引理 1** 命

$$g(x) = \exp\left(-x + \int_0^x \frac{\mathrm{e}^{-t} - 1}{t} \mathrm{d}t\right) \tag{4}$$

(此处 $\exp(y)$ 就是 $\mathrm{e}^y$). 这一函数有下列之性质:

(i) $g(x) = \dfrac{\mathrm{d}}{\mathrm{d}x}(x\mathrm{e}^x g(x))$;

(ii) $\displaystyle\int_0^\infty g(x)\mathrm{d}x = \mathrm{e}^{-\gamma}$.

---

① 1951 年 8 月 15 日收到. 发表于*Sci. Sinica*, 1951, 4: 393-402.

**证明** 求微分

$$\frac{\mathrm{d}}{\mathrm{d}x}(x\mathrm{e}^x g(x)) = \frac{\mathrm{d}}{\mathrm{d}x}\left(x\ \exp\int_0^x \frac{\mathrm{e}^{-t}-1}{t}\mathrm{d}t\right) = \exp\left(\int_0^x \frac{\mathrm{e}^{-t}-1}{t}\mathrm{d}t\right)\left(1+x\frac{\mathrm{e}^x-1}{x}\right) = g(x).$$

此式由 0 到 $\infty$ 的积分是

$$\int_0^\infty g(x)\mathrm{d}x = [x\mathrm{e}^x g(x)]_0^\infty = \left[x\ \exp\left(\int_0^x \frac{\mathrm{e}^{-t}-1}{t}\mathrm{d}t\right)\right]_0^\infty = \lim_{x\to\infty}\exp\left(\int_0^x \frac{\mathrm{e}^{-t}-1}{t}\mathrm{d}t+\log x\right) = \mathrm{e}^{-\gamma}.$$

关于最后一式, 读者可由熊庆来著《高等算学分析》第 359 页 (13) 式推得之.

**引理 2** 命

$$h(u) = \int_0^\infty g(x)\mathrm{e}^{-ux}\mathrm{d}x. \tag{5}$$

此积分当 $u>-1$ 时绝对收敛, 对 $u\geqslant -1+\varepsilon$ 时一致收敛. 此函数有下列诸性质:

(i) $h(0)=\mathrm{e}^{-\gamma}$;

(ii) $\lim\limits_{u\to\infty} uh(u)=1$;

(iii) $uh'(u-1)+h(u)=0$, 当$u>0$,

及

(iv) $uh(u-1)+\displaystyle\int_{u-1}^u h(t)\mathrm{d}t=1$, 当$u>0$.

**证明** (i) 式可由 Abel 定理及引理 1(ii) 得之. 命 $ux=y$, 则

$$uh(u)=\int_0^\infty g\left(\frac{y}{u}\right)\mathrm{e}^{-y}\mathrm{d}y,$$

易得结论 (ii) 在积分号下求微分, 由 (5) 式可知

$$\begin{aligned} uh'(u-1) &= -u\int_0^\infty g(x)\mathrm{e}^{-(u-1)x}x\mathrm{d}x \\ &= \int_0^\infty x\mathrm{e}^x g(x)\mathrm{d}(\mathrm{e}^{-ux}) \\ &= [x\mathrm{e}^x g(x)\mathrm{e}^{-ux}]_0^\infty - \int_0^\infty \mathrm{e}^{-ux}\mathrm{d}(x\mathrm{e}^x g(x)) \\ &\quad \text{(部分积分法)} \\ &= -\int_0^\infty \mathrm{e}^{-ux}g(x)\mathrm{d}x = -h(u) \end{aligned}$$

(引理 1(i)), 此即证明结论 (iii).

今先证明

$$q(u)=uh(u-1)+\int_{u-1}^{u}h(t)\mathrm{d}t$$

是一常数. 求此式之微分, 由 (iii) 可得

$$q'(u)=h(u-1)+uh'(u-1)+h(u)-h(u-1)=0,$$

故 $q(u)$ 是一常数. 命 $u\to\infty$, 则由 (ii) 可知

$$\lim_{u\to\infty}q(u)=1.$$

故得 (iv) 式.

**引理 3** 当 $u\geqslant 2$ 时, 有下列之恒等式:

$$\int_{u-1}^{u}\omega(t)h(t)\mathrm{d}t+u\omega(u)h(u-1)=\mathrm{e}^{-\gamma}.$$

**证明** 以 $p(u)$ 表示此式之左边, 先证 $p(u)$ 是常数. 由 (1) 及引理 2(iii), 可得

$$\begin{aligned}p'(u)=&\,\omega(u)h(u)-\omega(u-1)h(u-1)\\&+\frac{\mathrm{d}}{\mathrm{d}u}(u\omega(u))h(u-1)+u\omega(u)h'(u-1)=0.\end{aligned}$$

故 $p(u)$ 是常数. 而由 (1) 可知

$$\begin{aligned}p(2)=&\int_{1}^{2}\omega(t)h(t)\mathrm{d}t+2\omega(2)h(1)\\=&\int_{1}^{2}\frac{h(t)}{t}\mathrm{d}t+h(1)\\=&-\int_{1}^{2}h'(t-1)\mathrm{d}t+h(1)\qquad\text{(用引理 2(iii))}\\=&h(0)=\mathrm{e}^{-\gamma}.\qquad\text{(用引理 1(i))}\end{aligned}$$

**引理 4** 命

$$W(u)=\omega(u)-\mathrm{e}^{-\gamma},\tag{6}$$

则当 $u>0$ 时,

$$W(u)=-\frac{1}{uh(u-1)}\int_{u-1}^{u}W(t)h(t)\mathrm{d}t.\tag{7}$$

**证明** 由引理 3 及引理 2(iv) 可知

$$\int_{u-1}^{u}\omega(t)h(t)\mathrm{d}t+u\omega(u)h(u-1)=\mathrm{e}^{-\gamma}\left(\int_{u-1}^{u}h(t)\mathrm{d}t+uh(u-1)\right),$$

故得

$$\int_{u-1}^{u} W(t)h(t)\mathrm{d}t + uh(u-1)W(u) = 0.$$

此即 (7) 式.

命

$$F(u) = |W(u)|.$$

由 (7) 可得

$$\begin{aligned} F(u) \leqslant & \frac{1}{uh(u-1)} \int_{u-1}^{u} F(t)h(t)\mathrm{d}t \\ = & \frac{1}{uh(u-1)} \int_{0}^{1} F(u-1+\vartheta)h(u-1+\vartheta)\mathrm{d}\vartheta \\ \leqslant & \frac{1}{u} \int_{0}^{1} F(u-1+\vartheta)\mathrm{d}\vartheta \end{aligned} \tag{8}$$

(因为 $h(u)$ 显然是一单调递减函数).

**引理 5** 如果 $F(u)$ 是一正函数, 且当 $u$ 充分大时 $F(u)$ 适合 (8) 式, 则当 $u \to \infty$ 时,

$$F(u) \leqslant \mathrm{e}^{-u(\log u + \log\log u + \log\log u/\log u - 1) + O(u/\log u)}.$$

**证明** 为了使读者易于了解起见, 在证明中明确地引下"逐步求精法", 并且避免引用 Stirling 公式之类, 不然这证明是可以大大的缩短的.

1. 命

$$M(u) = \max_{u \leqslant x \leqslant \infty} F(x),$$

由 (8) 式立刻得出

$$M(u) \leqslant \frac{M(u-1)}{u} \leqslant \frac{M(u-2)}{u(u-1)} \leqslant \cdots = O\left(\frac{1}{P(u)}\right),$$

此处

$$\log P(u) = \log u + \log(u-1) + \cdots.$$

因为 $\log x$ 是递增函数, 所以

$$\log P(u) \geqslant \int_{1}^{u} \log x \mathrm{d}x = u(\log u - 1).$$

故得出

$$M(u) = O(\mathrm{e}^{-u(\log u - 1)}). \tag{9}$$

2. 命

$$F_1(u) = F(u)e^{u(\log u-1)},$$

$$M_1(u) = \max_{u\leqslant x\leqslant\infty} F_1(x).$$

由 (8) 式立刻得出

$$\begin{aligned} M_1(u) &\leqslant \frac{M_1(u-1)}{u}\int_0^1 \frac{e^{u(\log u-1)}}{e^{(u-1+t)(\log(u-1+t)-1)}}dt \\ &= \frac{M_1(u-1)}{u}\int_0^1 \exp(\varPhi(t))dt, \end{aligned} \tag{10}$$

此处

$$\begin{aligned} \varPhi(t) &= u(\log u-1)-(u+t-1)(\log(u+t-1)-1) \\ &\leqslant u(\log u-1)-(u+t-1)(\log(u-1)-1) \\ &= \log u-1+(u-1)(\log u-\log(u-1))-t(\log(u-1)-1) \\ &\leqslant \log u-t(\log(u-1)-1). \end{aligned}$$

代入 (10) 式, 立得

$$M_1(u)\leqslant M_1(u-1)\int_0^1 e^{-t(\log(u-1)-1)}dt\leqslant \frac{M_1(u-1)}{\log(u-1)-1}.$$

续用此式, 可知

$$M_1(u) = O\left(\frac{1}{P_1(u)}\right),$$

而

$$\begin{aligned} \log P_1(u) &= \log(\log(u-1)-1)+\log(\log(u-2)-1)+\cdots \\ &\geqslant \int^{u-1}\log(\log t-1)dt \\ &= \left[t\log(\log t-1)-\int\frac{dt}{\log t-1}\right]^{u-1} \\ &= u\log\log u - C_1\frac{u}{\log u}, \end{aligned}$$

此处 $C_1$ 是一常数 $>1$.

总之, 已证得

$$F(u)=O(\mathrm{e}^{-x(\log u+\log\log u-1)+C_1u/\log u}). \tag{11}$$

此结果已较Бухштаб的精密些, 但吾人仍能继续深入.

3. 命

$$F_2(u)=F_1(u)\mathrm{e}^{u\log\log u-C_1u/\log u},$$

及

$$M_2(u)=\max_{u\leqslant x\leqslant\infty}F_2(x).$$

由 (8) 式立刻得出

$$M_2(u)\leqslant\frac{M_2(u-1)}{u}\int_0^1\exp(\varPhi(t))\mathrm{d}t, \tag{12}$$

此处

$$\begin{aligned}
\varPhi(t)-\log u=&-\log u+u(\log u+\log\log u-1)\\
&-C_1u/\log u-(u+t-1)(\log(u+t-1)\\
&+\log\log(u+t-1)-1)+C_1\frac{u+t-1}{\log(u+t-1)}\\
\leqslant&(u-1)\log u+u\log\log u-C_1u/\log u-(u+t-1)(\log(u-1)\\
&+\log\log(u-1)-1)+C_1\frac{u+t-1}{\log(u-1)}\\
=&(u-1)\log\frac{u}{u-1}+\log\log u\\
&+(u-1)\log\left(\frac{\log u}{\log(u-1)}\right)-1-C_1\left(\frac{u}{\log u}-\frac{u-1}{\log(u-1)}\right)\\
&-t\left(\log(u-1)+\log\log(u-1)-1-\frac{C_1}{\log(u-1)}\right)\\
\leqslant&\log\log u+(u-1)\frac{1}{u-1}\\
&+(u-1)\frac{1}{(u-1)\log(u-1)}-1\\
&-\frac{C_1}{\log(u-1)}-t\left(\log u+\log\log u-1-\frac{C_1}{\log(u-1)}\right)\\
&(\text{此处用上了 }\log(1+x)\leqslant x)\\
\leqslant&\log\log u-t(\log u+\log\log u-2)+\frac{1}{\log(u-1)}
\end{aligned}$$

(当 $u$ 充分大时). 代入 (2) 式, 可知

$$\begin{aligned}M_2(u) \leqslant & M_2(u-1)\frac{\mathrm{e}^{\frac{1}{\log(u-1)}}\log u}{\log u+\log\log u-2}\\ \leqslant & M_2(u-1)\exp\left(-\log\left(1+\frac{\log\log u}{\log u}-\frac{2}{\log u}\right)+\frac{1}{\log(u-1)}\right)\\ \leqslant & M_2(u-1)\exp\left(-\frac{\log\log u}{\log u}+\frac{C_2}{\log u}\right)\end{aligned}$$

(因为 $\log(1+x)\geqslant x-Cx^2$). 又

$$\begin{aligned}&\frac{\log\log u}{\log u}-\frac{C_2}{\log u}+\frac{\log\log(u-1)}{\log(u-1)}-\frac{C_2}{\log(u-1)}+\cdots\\ \geqslant & \int^{u-1}\frac{\log\log t}{\log t}\mathrm{d}t-C_2\int^{u}\frac{\mathrm{d}t}{\log t}\\ \geqslant & \frac{u\log\log u}{\log u}-C_3\frac{u}{\log u}.\end{aligned}$$

故得出

$$M_2(u)\leqslant \mathrm{e}^{u\log\log u/\log u-C_3u/\log u},$$

即得

$$F(u)\leqslant \mathrm{e}^{-u(\log u+\log\log u+\log\log u/\log u-1)+C_4u/\log u}.$$

**附记**　此法并未尽其用, 还可以重复应用, 以得出更精密的结果.

综合引理 5、引理 4 及 (6) 可得下述

**定理**　$|\omega(u)-\mathrm{e}^{-\gamma}|\leqslant \mathrm{e}^{-u(\log u+\log\log u+\log\log u/\log u-1)+O(u/\log u)}$.

如果仅以证出

$$\lim_{u\to\infty}\omega(u)=\mathrm{e}^{-\gamma}$$

为满足, 我们有下列的简捷方法, 不过我们需引用 Laplace 积分的若干定理. 命

$$f(s)=\int_0^{\infty}\mathrm{e}^{-us}\mathrm{d}\alpha(u)=\int_0^{\infty}\mathrm{e}^{-us}\mathrm{d}\omega(u+1), \tag{13}$$

此处 $\alpha(u)=\omega(u+1)-1$. 由部分积分法可得

$$f(s)=s\int_0^{\infty}\mathrm{e}^{-us}\alpha(u)\mathrm{d}u$$

$$= -1 + s\int_0^\infty \mathrm{e}^{-us}\omega(u+1)\mathrm{d}u$$

$$= -1 + s\int_0^\infty \mathrm{e}^{-us}\mathrm{d}((u+2)\omega(u+2)).$$

换 $u$ 为 $u-1$, 用 (1) 式可知

$$f(s) = -1 + s\mathrm{e}^s\int_0^\infty \mathrm{e}^{-us}\mathrm{d}((u+1)\omega(u+1))$$

$$= -1 + s\mathrm{e}^s\left[\int_0^\infty \mathrm{e}^{-us}(u+1)\mathrm{d}\omega(u+1) + \int_0^\infty \mathrm{e}^{-us}\omega(u+1)\mathrm{d}u\right]. \tag{14}$$

积分号下求微分, 可得

$$\int_0^\infty u\mathrm{e}^{-us}\mathrm{d}\omega(u+1) = -f'(s),$$

部分积分可得

$$\int_0^\infty \mathrm{e}^{-us}\omega(u+1)\mathrm{d}u = -\frac{\mathrm{e}^{-us}}{s}\omega(u+1)\Big|_0^\infty + \frac{1}{s}\int_0^\infty \mathrm{e}^{-us}\mathrm{d}\omega(u+1)$$

$$=\frac{1}{s} + \frac{1}{s}f(s).$$

以此二式代入 (14), 可得

$$f(s) = -1 + s\mathrm{e}^s\left[f(s) - f'(s) + \frac{1}{s} + \frac{1}{s}f(s)\right],$$

即得一次常微分方程式

$$f'(s) + (s^{-1}(\mathrm{e}^{-s}-1)-1)f(s) = s^{-1}(1-\mathrm{e}^{-s}). \tag{15}$$

因为 $\lim\limits_{u\to 0}\alpha(u) = \lim\limits_{u\to 0}(\omega(u+1)-1) = 0$, 故由 Abel 定理 (例如 [4], p.183, Cor. 1c), 可知

$$\lim_{s\to\infty} f(s) = 0. \tag{16}$$

解一级线性微分方程式 (15) 并且条件 (16) 可得

$$f(s) = -\mathrm{e}^{s+\int_0^s t^{-1}(1-\mathrm{e}^{-t})\mathrm{d}t}\int_s^\infty \mathrm{e}^{-u-\int_0^u t^{-1}(1-\mathrm{e}^{-t})\mathrm{d}t}\frac{1-\mathrm{e}^{-u}}{u}\mathrm{d}u$$

$$=\mathrm{e}^{s+\int_0^5 t^{-1}(1-\mathrm{e}^{-t})\mathrm{d}t}\int_s^\infty \mathrm{e}^{-u-\int_0^u t^{-1}(1-\mathrm{e}^{-t})\mathrm{d}t}\mathrm{d}\left(-u - \int_0^u t^{-1}(1-\mathrm{e}^{-1})\mathrm{d}t\right)$$

$$
\begin{aligned}
&+ e^{s+\int_0^s t^{-1}(1-e^{-t})dt}\int_s^{\infty} e^{-u-\int_0^u t^{-1}(1-e^{-t})dt}du \\
&= -1 + e^{s+\int_0^s t^{-1}(1-e^{-t})dt}\int_s^{\infty} e^{-u-\int_0^u t^{-1}(1-e^{-t})dt}du \\
&= -1 + e^{s+\int_0^s t^{-1}(1-e^{-t})dt}[ue^{-\int_0^u t^{-1}(1-e^{-t})dt}]_s^{\infty} \\
&= -1 - se^s + e^{-\gamma+s+\int_0^s t^{-1}(1-e^{-t})dt}. \qquad (17)
\end{aligned}
$$

显然可得 $\lim\limits_{s\to 0} f(s) = -1 + e^{-\gamma}$. 由 Tauber 形定理可得

$$\lim_{u\to\infty}\alpha(u) = \lim_{u\to\infty}(\omega(u+1)-1) = -1+e^{-\gamma},$$

即所求之

$$\lim_{u\to\infty}\omega(u) = e^{-\gamma}.$$

但用 Tauber 形定理时必须注意 Tauber 形条件, 即

$$\int_0^t u d\alpha(u) = O(t) \qquad (\text{例如 [4], p.18, Thm.36}).$$

由

$$d\omega(u) = \frac{1}{u}(\omega(u-1)-\omega(u))du$$

可得

$$
\begin{aligned}
\int_0^t u d\alpha(u) &= \int_0^t u d\omega(u+1) \\
&= \int_1^t [\omega(u)-\omega(u+1)]du + O(1) \\
&= -\int_t^{t+1}\omega(u)du + O(1) = O(1)
\end{aligned}
$$

(易证 $\omega(u)=O(1)$). 故 Tauber 形条件适合. 定理完全证明.

以上证明有一堪注意之处, 即我们已求出 $\omega(u+1)$ 的 Laplace 变换式, 即 (17) 式.

## 参 考 文 献

[1] Бухштаб А А. Асимптотичеcкая оценка одной общей теоретико-числовой Функции. матем. сб., 1937, 2(144): 1239–1246.

[2] De Bruijn N G. On the number of uncancelled elements in the sieve of Eratoshens. *Nederl. Akad. Wetensch. Proc.*, 1950, 52: 803-812; *Indagationes Mathematicae*, 1950, 12: 247-256.

[3] Бухштаб А А. об асимптотической оценке числа чисел ариФметической прогрессии, неделящихся на《относительно》малые простые числа. матем. сб., 1951, 28(70): 166-184.

[4] Widder D V. The Laplace Tranaform.

(潘承彪 校)

# TARRY 问题的解数①

华罗庚 (清华大学和中国科学院)

## 1. 引　　言

设 $k \geqslant 2$ 及 $t_0$ 是整数, 它依赖于 $k$, 且由下表确定:

| $k$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | $>10$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $t_0$ | 3 | 8 | 23 | 62 | 156 | 380 | 889 | 2034 | 4595 | $[k^2(3\log k+\log\log k+4)]$ |

设 $r_t(P)$ 是下述丢番图方程组的解数:

$$\begin{gathered} x_1^k + \cdots + x_t^k = y_1^k + \cdots + y_t^k, \\ \cdots\cdots \\ x_1 + \cdots + x_t = y_1 + \cdots + y_t, \end{gathered} \tag{1.1}$$

并满足条件

$$1 \leqslant x_i, y_i \leqslant P. \tag{1.2}$$

本文的目的之一是证明: 当 $t > t_0$ 时, 有

$$\lim_{p\to\infty} p^{\frac{1}{2}k(k+1)-2t} r_t(P) = \vartheta_0 \mathfrak{S}, \tag{1.3}$$

其中

$$\vartheta_0 = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \left| \int_0^1 \mathrm{e}^{2\pi \mathrm{i}(\beta_k x^k + \cdots + \beta_1 x)} \mathrm{d}x \right|^{2t} \mathrm{d}\beta_k \cdots \mathrm{d}\beta_1, \tag{1.4}$$

$$\mathfrak{S} = \sum_{q_1=1}^{\infty} \cdots \sum_{q_k=1}^{\infty} \sum_{\substack{h_1=1 \\ (h_1,q_1)=1}}^{q_1} \cdots \sum_{\substack{h_k=1 \\ (h_k,q_k)=1}}^{q_k} \left| q_1^{-1} \cdots q_k^{-1} \sum_{x=1}^{q_1\cdots q_k} e\left(\frac{h_k}{q_k} x^k + \cdots + \frac{h_1}{q_1} x\right) \right|^{2t}. \tag{1.5}$$

本文中把 $\mathrm{e}^{2\pi \mathrm{i}x}$ 简记为 $e(x)$.

1939 年, 作者 [1] 证明了: 当

$$t > \frac{1}{4}k(k+1)\left(\left[\frac{6\log k + 2\log\log 2k + \log 23.2}{-\log\left(1-\dfrac{1}{k}\right)}\right] + k + 1\right) \tag{1.6}$$

① 1952 年 5 月 31 日收到. 发表于 *Acta Sci. Sinica*, 1952, 1: 1-76.

时式 (1.3) 成立, 对大的 $k$ 上式右边近似于 $1.5k^3\log k$(发表于1947年). 利用 Vinogradov[5] 的新方法和作者 [2] 的一个结果使我们能得到这一新改进.

设 $M(k)$ 是最小可能的整数 $t$ 便得方程组

$$x_1^h+\cdots+x_t^k=y_1^h+\cdots+y_t^h,\quad 1\leqslant h\leqslant k,$$
$$x_1^{k+1}+\cdots+x_t^{k+1}\neq y_1^{k+1}+\cdots+y_t^{k+1}$$

可解. 由式 (1.3) 显然可得

$$M(k)\leqslant t_0+1.$$

作者 [3] 早先得到一个结果是

$$M(k)\geqslant(k+1)\left(\left[\frac{\log\frac{1}{2}(k+2)}{\log(k+1)-\log k}\right]+1\right)\quad(\sim k^2\log k,\text{对大的}k).$$

这两个估计的差别仅是一个常数因子. 这显示了本方法的强有力.

特别还应注意的是实密度 $\partial_0$ 及 $p$-adic 密度 $\partial_p$(它是我们的奇异级数的一个因子) 的收敛性问题. 为了处理 $\partial_0$ 的收敛性问题, 作者利用了多重 Fourier 积分的 Young-Hausdorff 定理. 这样所得到的收敛指数要强于早先从指数积分估计[6] 所得到的. 最佳可能的指数仍是一个未解决的问题.

对 $p$-adic 密度及 $\mathfrak{S}$ 的收敛性. 作者引进了一个新方法, 由此得到了收敛指数的最佳可能的值.

本文独立于作者的俄文著作[1]. 除了早先的两篇文章[3,4] 外, 本文是完整自封的.

全文中我们用 $\varepsilon$ 表示任意小的正数, 在不同的地方可以是不同的. 用 $c_1,c_2,\cdots$ 表示仅与 $k,\varepsilon$ 及有时与 $t$ 有关的常数. 符号大 $O$ 中包含的常数就是这些 $c$.

## 2. 常 数 $\vartheta_0$

以 $D_0$ 表示区域

$$0\leqslant x_1<x_2<x_3<\cdots<x_k\leqslant 1.$$

变量 $y_1,\cdots,y_k$ 的区域 $D$ 是 $D_0$ 在映射

$$y_h=x_1^h+\cdots+x_k^h,\quad h=1,\cdots,k \tag{2.1}$$

下的象. 这映射的 Jacobi 行列式是

$$\frac{\partial(y_1,\cdots,y_k)}{\partial(x_1,\cdots,x_k)}=k!\prod_{1\leqslant i<j\leqslant k}(x_j-x_i), \tag{2.2}$$

当 $(x_1,\cdots,x_k)$ 属于 $D_0$ 时, 它是正的.

定义 $y=(y_1,\cdots,y_k)$, 及

$$f(y_1,\cdots,y_k)=\begin{cases}\dfrac{1}{k!\displaystyle\prod_{1\leqslant i<j\leqslant k}(x_j-x_i)}, & y\in D;\\ 0, & \text{其他}.\end{cases} \tag{2.3}$$

显见, $f(y_1,\cdots,y_k)$ 在一有限区域外为零 (即在区域

$$0\leqslant y_h\leqslant k,\quad h=1,2,\cdots,k$$

外为零). 函数 $f(y_1,\cdots,y_k)$ 的 Fourier 变换是①

$$\begin{aligned}&\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}f(y_1,\cdots,y_k)e(\gamma_1y_1+\cdots+\gamma_ky_k)\mathrm{d}y_1\cdots\mathrm{d}y_k\\ =&\int\cdots\int_D f(y_1,\cdots,y_k)e(\gamma_1y_1+\cdots+\gamma_ky_k)\mathrm{d}y_1\cdots\mathrm{d}y_k\\ =&\int\cdots\int_{D_0} e(\gamma_k(x_1^k+\cdots+x_k^k)+\cdots+\gamma_1(x_1+\cdots+x_k))\mathrm{d}x_1\cdots\mathrm{d}x_k\\ =&\frac{1}{k!}\int_0^1\cdots\int_0^1 e(\gamma_k(x_1^k+\cdots+x_k^k)+\cdots+\gamma_1(x_1+\cdots+x_k))\mathrm{d}x_1\cdots\mathrm{d}x_k\\ =&\frac{1}{k!}\left(\int_0^1 e(\gamma_kx^k+\cdots+\gamma_1x)\mathrm{d}x\right)^k.\end{aligned} \tag{2.4}$$

这就是说,

$$\frac{1}{k!}\left(\int_0^1 e(\gamma_kx^k+\cdots+\gamma_1x)\mathrm{d}x\right)^k \tag{2.5}$$

是一个在一有限区域外为零的函数的 Fourier 变换. 不幸的是, $f(y_1,\cdots,y_k)$ 不属于 $L^2$. 若是这样, 我们就可利用 Parseval 关系式来得到当 $t=k$ 时 $D_0$ 的值. 尽管如此, 我们有以下结论:

**引理 2.1** 函数 $f(y_1,\cdots,y_k)$ 属于 $L^\sigma$, 当 $\sigma<1+\frac{2}{k}$, 以及它不属于 $L^\sigma$, 当 $\sigma>1+\frac{2}{k}$.

---

① 与常用记号的一个小差别是, 我们用 $g(x)=\int_{-\infty}^{\infty}f(y)e(xy)\mathrm{d}y$ 表示 $f(y)$ 的 Fourier 变换, 这时反转公式应是 $f(y)=\int_{-\infty}^{\infty}g(x)e(-yx)\mathrm{d}x$.

**证明** 我们有

$$I = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} |f(y_1, \cdots, y_k)|^{\sigma} \mathrm{d}y_1 \cdots \mathrm{d}y_k$$
$$= \underset{D_0}{\int \cdots \int} \left( k! \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i) \right)^{1-\sigma} \mathrm{d}x_1 \cdots \mathrm{d}x_k. \tag{2.6}$$

当 $\sigma \leqslant 1$ 时引理显然成立, 以及当 $\sigma \geqslant 2$ 时积分 (2.6) 显然发散. 现在来考虑取值范围

$$1 < \sigma < 2. \tag{2.7}$$

设

$$x_k = x_{k-1} + \delta_{k-1}, x_{k-1} = x_{k-2} + \delta_{k-2}, \cdots, x_2 = x_1 + \delta_1.$$

区域 $D_0$ 就变为

$$0 \leqslant \delta_1, 0 \leqslant \delta_2, \cdots, 0 \leqslant \delta_{k-1}, \delta_1 + \cdots + \delta_{k-1} \leqslant 1 \tag{2.8}$$

及

$$0 \leqslant x_1 \leqslant 1 - \delta_1 - \cdots - \delta_{k-1},$$

因为 $x_k = \delta_1 + \cdots + \delta_{k-1} + x_1$. 设 $D'$ 是由式 (2.8) 确定的 $(k-1)$ 维区域. 这样就有

$$\begin{aligned} I =& k!^{1-\sigma} \underset{D'}{\int \cdots \int} (\delta_1 \cdots \delta_{k-1} (\delta_1 + \delta_2)(\delta_2 + \delta_3) \\ & \cdots (\delta_{k-2} + \delta_{k-1})(\delta_1 + \delta_2 + \delta_3) \cdots (\delta_1 + \cdots + \delta_{k-1}))^{1-\sigma} \\ & \times (1 - \delta_1 - \cdots - \delta_{k-1}) \mathrm{d}\delta_1 \cdots \mathrm{d}\delta_{k-1} \\ \leqslant & k!^{1-\sigma} \sum_{\lambda_1 + \cdots + \lambda_{k-1} = \frac{1}{2}k(k-1)} \underset{D'}{\int \cdots \int} (\delta_1^{\lambda_1} \cdots \delta_{k-1}^{\lambda_{k-1}})^{1-\sigma} \\ & \times (1 - \delta_1 - \cdots - \delta_{k-1}) \mathrm{d}\delta_1 \cdots \mathrm{d}\delta_{k-1}, \end{aligned} \tag{2.9}$$

因为 $(A+B)^{1-\sigma} \leqslant A^{1-\sigma} + B^{1-\sigma}$, 当 $1 \leqslant \sigma < 2$ 及 $A \geqslant 0, B \geqslant 0$.

式 (2.9) 中的每个积分是 Dirichlet 积分, 作变量替换后就变为单重积分

$$\int_0^1 \tau^{\frac{1}{2}k(k-1)(1-\sigma)+k-2}(1-\tau)\mathrm{d}\tau,$$

这积分是收敛的, 当

$$\frac{1}{2}k(k-1)(1-\sigma) + k - 1 > 0,$$

或

$$\sigma < 1 + \frac{2}{k}.$$

现在来证明积分 (2.6), 当 $\sigma > 1 + \frac{2}{k}$ 时是发散的. 设 $0 < \delta < \frac{1}{k}$. 显见, 这积分大于

$$k!^{1-\sigma} \int_{k\delta}^{1} \mathrm{d}x_k \int_{x_k-\delta}^{x_k} \mathrm{d}x_{k-1} \cdots \int_{x_2-\delta}^{x_2} \left( \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i) \right)^{1-\sigma} \mathrm{d}x_1$$

$$\geqslant (k!(k-1)!(k-2)! \cdots 1)^{1-\sigma} \int_{k\delta}^{1} \mathrm{d}x_k \int_{x_k-\delta}^{x_k} \mathrm{d}x_{k-1} \cdots \int_{x_2-\delta}^{x_2} \delta^{\frac{1}{2}(1-\sigma)k(k-1)} \mathrm{d}x_1,$$

因为 $x_i - x_j \leqslant (i-j)\delta$ 当 $i > j$. 所以

$$I > c_1 \delta^{k-1+\frac{1}{2}(1-\sigma)k(k-1)},$$

若 $\sigma > 1 + \frac{2}{k}$, 上式右边趋于无穷, 当 $\delta \to 0$.

**注** 看来 $f(y_1, \cdots, y_k)$ 应不属于 $L^{1+\frac{2}{k}}$. 当 $k = 2$ 和 $k = 3$ 时, 可计算 $I$ 的值, 它们分别是

$$\frac{2^{1-\sigma}}{(2-\sigma)(3-\sigma)} = 2^{1-\sigma} \frac{\Gamma(2-\sigma)}{\Gamma(4-\sigma)},$$

$$(3 \cdot 2)^{1-\sigma} \frac{(\Gamma(2-\sigma))^2 \Gamma(5-3\sigma)}{\Gamma(4-2\sigma)\ \Gamma(7-3\sigma)}.$$

利用 Fourier 积分的 Young-Hausdorff 定理可得

**引理 2.2** 积分

$$\int_0^1 \mathrm{e}(\gamma_k x^k + \cdots + \gamma_1 x) \mathrm{d}x \tag{2.10}$$

属于 $L^{\frac{1}{2}k(k+2)+\varepsilon}$.

**证明** Young-Hausdorff 定理断言: 若 $f$ 属于 $L^p(1 < p \leqslant 2)$, 则它的 Fourier 变换属于 $L^{p'}, p' = \frac{p}{(p-1)}$. 现取 $p = \sigma < 1 + \frac{2}{k}$, 则 $p' > \frac{k}{2} + 1$. 这就是说, 积分 (2.5) 属于 $L^{\frac{k}{2}+1+\varepsilon}$. 因此, 积分 (2.10) 属于 $L^{\frac{k(k+2)}{2}+\varepsilon}$.

**注** 1. 最佳可能的指数值是一个未解决的问题.

2. 若把积分 (2.10) 看作是单变量 $\gamma_u (1 \leqslant u \leqslant k)$ 的函数, 那么利用同样的方法可推出积分 (2.10) 属于 $L^{u+\varepsilon}$. 证明是十分相似的. 因为相应于 $\gamma_u$ 的积分 (2.10) 的 Fourier 变换是

$$f(y) = \begin{cases} e(\gamma_k y^{\frac{k}{u}} + \cdots + \gamma_{u+1} y^{\frac{u-1}{u}} + \gamma_{u-1} y^{\frac{u+1}{u}} + \cdots + \gamma_1 y^{\frac{1}{u}}) y^{\frac{1}{u}-1}, & 0 \leqslant y \leqslant 1, \\ 0, & \text{其他}. \end{cases} \tag{2.11}$$

显见, 当 $\sigma < 1+\dfrac{1}{(u-1)}$ 时, 由式 (2.11) 给出的 $f(y)$ 属于 $L^{\sigma}$. 根据 Young-Hausdorff 定理, 积分 (2.10) 属于 $L^{u+\varepsilon}$. 这一点启示我们, 对大的 $\gamma$ 关于积分 (2.10) 的性质应有某些结论. 这正是下节所要讨论的.

## 3. 指数积分的估计

我们需要关于单重积分的一个引理.

**引理 3.1** 设 $\varphi(x)$ 是区间 $(a,b)$ 上的实函数, 有有限多个[①]极大值和极小值. 那么有

$$\int_a^b \varphi(x)e(x)\mathrm{d}x = 0\left(\max_{0\leqslant\varepsilon\leqslant 1}\max_{a\leqslant v\leqslant b-\varepsilon}\int_v^{v+\varepsilon}|\varphi(x)|\mathrm{d}x\right). \tag{3.1}$$

**证明** 当 $b-a\leqslant 1$ 时, 引理显然成立. 现假定 $a<b-1$. 我们只要证明

$$\int_a^b \varphi(x)e(x)\mathrm{d}x = O\left(\max_{a\leqslant v\leqslant b-1}\int_v^{v+1}|\varphi(x)|\mathrm{d}x\right). \tag{3.2}$$

无妨一般, 可假定$\varphi(x)$是单调的, 若不然, 可把区间分为有限个小区间, 使得在每个小区间上函数是单调的. 因为论证是完全类似的, 我们可假定$\varphi(x)$是递减的. 由于

$$\int_a^b \varphi(x)e(x)\mathrm{d}x \leqslant \int_a^{[a]+1}|\varphi(x)|\mathrm{d}x + \left|\int_{[a]+1}^{[b]}\varphi(x)e(x)\mathrm{d}x\right| + \int_{[b]}^b|\varphi(x)|\mathrm{d}x,$$

所以, 只要证明式 (3.2) 当 $a$ 和 $b$ 是整数时成立.

我们有

$$\begin{aligned}\int_a^b \varphi(x)\sin 2\pi x\mathrm{d}x &= \int_a^{a+\frac12}\varphi(x)\sin\ 2\pi x\mathrm{d}x + \int_{a+\frac12}^{a+1}\varphi(x)\sin\ 2\pi x\mathrm{d}x + \cdots\\ &= \int_0^{\frac12}(\varphi(x+a)-\varphi\left(x+a+\frac12\right)\\ &\quad +\varphi(x+a+1)-\cdots-\varphi\left(x+b-\frac12\right))\sin\ 2\pi x\mathrm{d}x,\end{aligned}$$

因 $\varphi(x)$ 是递减的, 故有

$$0\leqslant \varphi(x+a)-\varphi\left(x+a+\frac12\right)+\varphi(x+a+1)-\cdots-\varphi\left(x+b-\frac12\right)\leqslant\varphi(x+a).$$

因而得到

$$0\leqslant\int_a^b\varphi(x)\sin 2\pi x\mathrm{d}x\leqslant\int_0^{\frac12}\varphi(x+a)\sin\ 2\pi x\mathrm{d}x$$

① 我们说有限多个是指这个数仅依赖于 $k$.

$$\leqslant \int_0^{\frac{1}{2}} |\varphi(x+a)|\mathrm{d}x = \int_a^{a+\frac{1}{2}} |\varphi(x)|\mathrm{d}x.$$

对

$$\int_a^b \varphi(x)\cos 2\pi x\mathrm{d}x$$

可得类似结果. 综上所得就证明了引理.

**引理 3.2**　设 $\gamma_k, \cdots, \gamma_1$ 是 $k$ 个实数, 及

$$I = \int_0^1 e(\gamma_k x^k + \cdots + \gamma_1 x)\mathrm{d}x. \tag{3.3}$$

我们有

$$I = O(\min(1, |\gamma_1|^{-\frac{1}{k}}, \cdots, |\gamma_k|^{-\frac{1}{k}})). \tag{3.4}$$

**证明**　$|I| \leqslant 1$ 是显然的. 因而可假定 $|\gamma_i| \geqslant 1$. 我们有

$$I^k = \int_0^1 \cdots \int_0^1 e(\psi)\mathrm{d}x_1 \cdots \mathrm{d}x_k,$$

其中

$$\psi = (x_1^k + \cdots + x_k^k)\gamma_k + \cdots + (x_1 + \cdots + x_k)\gamma_1.$$

显有

$$I^k \leqslant k! \int\cdots\int_{0\leqslant x_k\leqslant x_{k-1}\leqslant\cdots\leqslant x_1\leqslant 1} e(\psi)\mathrm{d}x_1\cdots\mathrm{d}x_k. \tag{3.5}$$

我们考虑映射

$$\begin{aligned}(x_1^k + \cdots + x_k^k)|\gamma_k| &= y_k,\\ &\cdots\cdots\\ (x_1 + \cdots + x_k)|\gamma_1| &= y_1,\end{aligned} \tag{3.6}$$

并设 $R$ 是 $y_1, \cdots, y_k$ 的取值区域. 映射 (3.6) 的 Jacobi 行列式 $\dfrac{\partial(x_1,\cdots,x_k)}{\partial(y_1,\cdots,y_k)} = g(y_1,\cdots,y_k)$ 总是正的. 这样就有

$$\begin{aligned}|k!^{-1}I^k| =& \left|\int\cdots\int_R e(y_k+\cdots+y_1)g(y_1,\cdots,y_k)\mathrm{d}y_1\cdots\mathrm{d}y_k\right|\\ \leqslant& \int\cdots\int \mathrm{d}y_1\cdots\mathrm{d}y_{h-1}\mathrm{d}y_{h+1}\cdots\mathrm{d}y_k\left|\int e(y_h)g(y_1,\cdots,y_k)\mathrm{d}y_h\right|\\ =& O\Big(\max_{\substack{v\\0\leqslant\xi\leqslant 1}}\int\cdots\int \mathrm{d}y_1\cdots\mathrm{d}y_{h-1}\mathrm{d}y_{h+1}\cdots\mathrm{d}y_k\int_{v\leqslant y_h\leqslant v+\xi} g(y_1,\cdots,y_k)\mathrm{d}y_h\Big)\end{aligned}$$

$$=O\Big(\max_{0\leqslant\xi\leqslant 1}\underset{v\leqslant y_h\leqslant v+\xi}{\int_0^1\cdots\int_0^1}\mathrm{d}x_1\cdots\mathrm{d}x_k\Big), \tag{3.7}$$

这里用到了引理 3.1.

我们有

$$\underset{v\leqslant y_h\leqslant v+\xi}{\int_0^1\cdots\int_0^1}\mathrm{d}x_1\cdots\mathrm{d}x_k\leqslant\underset{v\leqslant y_h\leqslant v+\xi}{\int\cdots\int}\mathrm{d}x_1\cdots\mathrm{d}x_k\leqslant\underset{v\leqslant y_h\leqslant v+1}{\int\cdots\int}\mathrm{d}x_1\cdots\mathrm{d}x_k$$
$$=V(v+1)-V(v), \tag{3.8}$$

这里 $V(v)$ 是区域

$$y_h=|\gamma_h|(x_1^h+\cdots+x_k^h)\leqslant v,\quad x_v\geqslant 0$$

的体积. 因为

$$V(v)=\eta\Big(\frac{v}{|\gamma_h|}\Big)^{k/h},$$

其中 $\eta$ 是仅和 $k$ 及 $h$ 有关的常数, 故有

$$\begin{aligned}V(v+1)-V(v)=&O\bigg(\Big(\frac{v+1}{|\gamma_h|}\Big)^{k/h}-\Big(\frac{v}{|\gamma_h|}\Big)^{k/h}\bigg)\\=&O(|\gamma_h|^{-k/h}\int_v^{v+1}t^{k/h-1}\mathrm{d}t)\\=&O(|\gamma_h|^{-k/h}(v+1)^{k/h-1})\\=&O(|\gamma_h|^{-k/h}(|\gamma_h|k+1)^{k/h-1}),\end{aligned} \tag{3.9}$$

这里用到了 $v\leqslant k|\gamma_h|$. 综合式 (3.7),(3.8) 及 (3.9), 就推出

$$\begin{aligned}I^k=&O(|\gamma_h|^{-k/h}(|\gamma_h|k+1)^{k/h-1})\\=&O(|\gamma_h|^{-k/h-1+k/h})=O(|\gamma_h|^{-1}).\end{aligned}$$

这就证明了引理.

**注** 这引理是属于 Vinogradov 的, 但这里给出的证明是新的, 它提出了该结果中的某些可能的改进. 利用这引理也可证明一个有关积分 (2.10) 的收敛性的定理, 但它没有引理 2.2 那样好. 因为当 $A_v>0$ 时, $\min(A_k,\cdots,A_1)\leqslant(A_k\cdots A_1)^{1/k}$, 所以有

$$I=O(\min(1,|\gamma_k\cdots\gamma_1|^{-1/k^2})). \tag{3.10}$$

因而当 $2t\geqslant k^2+\varepsilon$ 时,

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|I|^{2t}\mathrm{d}\gamma_1\cdots\mathrm{d}\gamma_k$$

收敛, 即 $I$ 属于 $L^{k^2+\varepsilon}$.

## 4. 奇异级数

$\mathfrak{S}$ 称为 Tarry 问题的奇异级数. 如果它收敛, 则显然是正的. 这级数的收敛性可由下面的引理推出.

**引理 4.1**[4]　设 $a_k, \cdots, a_0$ 及 $q$ 是整数, 且 $q > 0$, 再设

$$g(x) = a_k x^k + \cdots + a_1 x + a_0, \tag{4.1}$$

$(a_k, \cdots, a_1, q) = 1$. 那么

$$\sum_{x=1}^{q} e(g(x)/q) = O(q^{1-1/k+\varepsilon}). \tag{4.2}$$

引理的证明见文献 [1, 4]. 利用 §6 – §8 的方法可给出引理的另一个证明, 实际上这是先前给出的证明的改进.

**引理 4.2**　当 $t > k^2$ 时奇异级数 $\mathfrak{S}$ 收敛.

**证明**　设 $Q$ 是 $q_1, \cdots, q_k$ 的最小公倍数. 那么有

$$\left(\frac{h_k Q}{q_k}, \cdots, \frac{h_1 Q}{q_1}, Q\right) = 1, \tag{4.3}$$

若不成立, 则有素数 $p$ 使得

$$p \left| \left(\frac{h_k Q}{q_k}, \cdots, \frac{h_1 Q}{q_1}, Q\right)\right. . \tag{4.4}$$

设 $b$ 是使得 $p^b$ 整除 $Q$ 的最大整数. 由 $Q$ 的定义知, $q_1, \cdots, q_k$ 中必有一个被 $p^b$ 整除, 设为 $q_l$. 但由式 (4.4) 知, $p$ 整除 $\frac{h_l}{q_l} Q$, 这推出 $p$ 整数 $h_l$, 这和 $(h_l, q_l) = 1$ 矛盾.

由引理 4.1 可得

$$\begin{aligned}
&\sum_{x=1}^{q_1 \cdots q_k} e\left(\frac{h_k}{q_k} x^k + \cdots + \frac{h_1}{q_1} x\right) \\
=&\frac{q_1 \cdots q_k}{Q} \sum_{x=1}^{Q} e(g(x)/Q) \\
=&O(q_1 \cdots q_k Q^{-1/k+\varepsilon}).
\end{aligned} \tag{4.5}$$

因而有

$$\mathfrak{S} = O\left(\sum_{q_1=1}^{\infty} \cdots \sum_{q_k=1}^{\infty} \sum_{h_1} \cdots \sum_{h_k} Q^{-2t/k+\varepsilon}\right)$$

$$=O\left(\sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}q_1\cdots q_k Q^{-2t/k+\varepsilon}\right). \tag{4.6}$$

因为 $Q\geqslant\max(q_1,\cdots,q_k)\geqslant(q_1\cdots q_k)^{1/k}$, 故有

$$\mathfrak{S}=O\left(\sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}(q_1\cdots q_k)^{1-2t/k^2+\varepsilon}\right),$$

上式右边的级数当 $t>k^2$ 时收敛.

**注** 事实上, 上面的方法能给出稍好一些的结果, 因为我们没有充分利用下面级数的性质:

$$\tau=\sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}q_1\cdots q_k Q^{-2t/k+\varepsilon}. \tag{4.7}$$

对固定的 $Q$, 考虑和

$$\sigma(Q)=\sum\cdots\sum q_1\cdots q_k, \tag{4.8}$$

这里是对所有最小公倍数为 $Q$ 的正整数组 $q_1,\cdots,q_k$ 求和.

设 $Q=p_1^{l_1}\cdots p_s^{l_s}$, 我们有

$$\sigma(Q)=\sum\cdots\sum(p_1^{l_{11}}\cdots p_s^{l_{1s}})(p_1^{l_{2l}}\cdots p_s^{l_{2s}})\cdots(p_1^{l_{kl}}\cdots p_s^{l_{ks}}),$$

这里是对所有满足下述条件的非负整数 $l_{ij}$ 求和:

$$\max(l_{1j},\cdots l_{kj})=l_j.$$

显有

$$\sigma(Q)=kQ(S(Q))^{k-1}, \tag{4.9}$$

这里 $S(Q)$ 是 $Q$ 的除数之和. 因为 $S(Q)=O(Q^{1+\varepsilon})$, 故有

$$\tau=\sum_{Q=1}^{\infty}\sigma(Q)Q^{-2t/k+\varepsilon}=k\sum_{Q=1}^{\infty}(S(Q))^{k-1}Q^{1-2t/k+\varepsilon}=O\left(\sum_{Q=1}^{\infty}Q^{k-2t/k+\varepsilon}\right),$$

最后一个级数当 $t>\frac{1}{2}k(k+1)$ 时收敛.

但这还不是最佳可能结果, 事实上, 利用更精细的方法可证明奇异级数当 $t>k(k+1)/4+1$ 时收敛. 反之, 先来证明.

**引理 4.3** 级数 $\mathfrak{S}$ 当 $t=k(k+1)/4+1$ 时发散.

**证明** 下面的级数是我们奇异级数的一部分.

$$\mathfrak{S}_1=\sum_{p>k}\sum_{\substack{h_k=1\\p\nmid h_k}}^{p^k}\cdots\sum_{\substack{h_1=1\\p\nmid h_1}}^{p}\sum_{c=1}^{p}\Big|p^{-1-\cdots-k}$$

$$\times \sum_{x=1}^{p^{1+\cdots+k}} e\left(\frac{h_k}{p^k}(x+c)^k+\cdots+\frac{h_1}{p}(x+c)\right)\Bigg|^{2t}$$

$$=\sum_{p}\sum_{h_k}\cdots\sum_{h_1} p\left|p^{-k}\sum_{x=1}^{p^k} e\left(\frac{h_k}{p^k}x^k+\cdots+\frac{h_1}{p}x\right)\right|^{2t}.$$

若能证明, 当 $p>k$ 时,

$$\sum_{x=1}^{p^k} e\left(\frac{h_k}{p_k}x^k+\cdots+\frac{h_1}{p}x\right)=p^{k-1}, \tag{4.10}$$

那么

$$\begin{aligned}\mathfrak{S} &=\sum_{p>k} p^{\frac{1}{2}k(k-1)}(p-1)^k p^{-2t+1}\\ &\geqslant\frac{1}{2^k}\sum_{p>k} p^{\frac{1}{2}k(k+1)-2t+1}\\ &\geqslant\frac{1}{2^k}\sum_{p} p^{-1},\end{aligned}$$

它是发散的.

我们来证明 (4.10). 设 $X=p^{k-1}y+z$, 我们有

$$\begin{aligned}&\sum_{x=1}^{p^k} e\left(\frac{h_k}{p^k}x^k+\cdots+\frac{h_1}{p}x\right)\\ =&\sum_{z=1}^{p^{k-1}} e\left(\frac{h_k}{p^k}z^k+\cdots+\frac{h_1}{p}z\right)\sum_{y=1}^{p} e\left(\frac{kh_k}{p}yz^{k-1}\right).\end{aligned}$$

除 $p$ 整除 $z$ 外, 上式的内层和必为零. 作替换 $z=pw$ 就得到式 (4.10).

为了确定 $t$ 的最佳上界, 我们需要奇异级数的一个更简洁的形式, 它将告诉我们奇异级数的算术意义.

## 5. 奇异级数的算术性状

**引理 5.1** 我们有

$$\mathfrak{S}=\sum_{Q=1}^{\infty}\sum_{(a_k,\cdots,a_1,Q)=1}\left|Q^{-1}\sum_{x=1}^{Q} e(a_kx^k+\cdots+a_1x)/Q\right|^{2t}, \tag{5.1}$$

这里 $a_1,\cdots,a_k$ 中的每一个均遍历模 $Q$ 的完全剩余系, 且满足 $(a_k,\cdots,a_1,Q)=1$.

**证明** 引理是下述事实的直接推论：对应

$$\frac{h_l Q}{q_l} = a_l, \quad l = 1, 2, \cdots, k,$$

其中 $Q$ 是 $q_1, \cdots, q_k$ 的最小公倍数, 是式 (1.5) 的求和范围：

$$q_l = 1, 2, 3, \cdots, \quad (h_l, q_l) = 1, \quad 1 \leqslant h_l \leqslant q_l, \quad l = 1, 2, \cdots, k$$

与式 (5.1) 的求和范围：

$$Q = 1, 2, 3, \cdots, \quad (a_k, \cdots, a_1, Q) = 1, \quad 1 \leqslant a_l \leqslant Q, \quad l = 1, \cdots, k$$

之间的一一对应. 这是一个几乎显然的事实. 由

$$q_1^{-1} \cdots q_k^{-1} \sum_{x=1}^{q_1 \cdots q_k} = Q^{-1} \sum_{x=1}^{Q}.$$

就推出引理.

**定义** 设 $N(p^\gamma)$ 是同余方程

$$x_1^h + \cdots + x_t^h \equiv y_1^h + \cdots + y_t^h (\bmod p^\gamma),$$
$$1 \leqslant h \leqslant k, \qquad 1 \leqslant x, y \leqslant p^\gamma$$

的解数.

**引理 5.2** 我们有

$$p^{-\gamma(2t-k)} N(p^\gamma) = \sum_{t=0}^{\gamma} \sum_{\substack{a_1=1 \\ p\nmid(a_1,\cdots,a_k)}}^{p^l} \cdots \sum_{a_k=1}^{p^l} \left| p^l \sum_{x=1}^{p^l} e((a_k x^k + \cdots + a_1 x)/p^l) \right|^{2t}. \tag{5.2}$$

**证明** 显有

$$\begin{aligned}
N(p^\gamma) &= \frac{1}{p^{\gamma k}} \sum_{a_1=1}^{p^\gamma} \cdots \sum_{a_k=1}^{p^\gamma} \left| \sum_{x=1}^{p^\gamma} e((a_k x^k + \cdots + a_1 x)/p^\gamma) \right|^{2t} \\
&= \frac{1}{p^{\gamma k}} \sum_{m=0}^{\gamma} \sum_{\substack{a_1=1 \\ (a_1,\cdots,a_k,p^\gamma)=p^m}}^{p^\gamma} \cdots \sum_{a_k=1}^{p^\gamma} \left| \sum_{x=1}^{p^\gamma} e((a_k x^k + \cdots + a_1 x)/p^\gamma) \right|^{2t} \\
&= \frac{1}{p^{\gamma k}} \sum_{m=0}^{\gamma} \sum_{\substack{b_1=1 \\ p\nmid(b_1,\cdots,b_k)}}^{p^{\gamma-m}} \cdots \sum_{b_k=1}^{p^{\gamma-m}} \left| p^m \sum_{x=1}^{p^{\gamma-m}} e((b_k x^k + \cdots + b_1 x)/p^{\gamma-m}) \right|^{2t}
\end{aligned}$$

$$=p^{2t\gamma-\gamma k}\sum_{l=0}^{\gamma}\sum_{\substack{b_1=1 \\ p\nmid(b_1,\cdots,b_k)}}^{p^l}\cdots\sum_{b_k=1}^{p^l}\left|p^l\sum_{x=1}^{p^l}e((b_kx^k+\cdots+b_1x)/p^l)\right|^{2t}.$$

这就证明了引理 5.2.

因为式 (5.2) 的右边是奇异级数的一部分, 所以由引理 4.2 知, 当 $t>k^2$ 时, 存在极限

$$\partial_p=\lim_{r\to\infty}p^{-\gamma(2t-k)}N(p^\gamma).$$

这称为是 Tarry 问题的 $p$-adic 密度. 由于 $\mathfrak{S}$ 的绝对收敛性, 容易证明当 $t>k^2$ 时有

$$\mathfrak{S}=\prod_p\partial p. \tag{5.3}$$

这就是奇异级数的算术性状. 在 §6 − §9, 我们将对 $t$ 的最佳可能的下界来证明式 (5.3).

## 6. 同余方程解的 $p$-adic 展开

设 $p$ 是给定的素数, $l>0$ 是给定的整数. 再设 $g_1(x)$ 是模 $p^l$ 的 $n$ 次整系数多项式, 以及 $r_0(\geqslant 0)$ 是使得 $p^{r_0}$ 整除 $g_1(x)$ 的所有系数的最大整数, 再设 $x'$ 是

$$p^{-r_0}g_1(x)\equiv 0(\bmod p),\quad 0\leqslant x'<p \tag{6.1}$$

的解. 记

$$g_2(x)=p^{-r_0}g_1(px+x'). \tag{6.2}$$

代替 $g_1(x)$ 和模 $p^l$ 我们来考虑 $g_2(x)$ 和模 $p^{l-r_0}$. 这样就有 $p$ 的最高方幂 $r_1$ 使得 $p^{r_1}$ 整除 $g_2(x)$ 的所有系数, 显有 $r_1\geqslant 1$. 设 $x''$ 是

$$p^{-r_1}g_2(x)\equiv 0(\bmod p),\quad 0\leqslant x''<p \tag{6.3}$$

的解及 $g_3(x)=p^{-r_1}g_2(px+x''), \bmod p^{l-r_0-r_1}$, 等等. 继续这样的步骤, 直至 $e$ 步后我们有 $r_0+\cdots+r_{e-1}=l$, 及 $g_e(x)$ 的所有系数被 $p^{l-r_1-\cdots-r_{e-2}}$ 整除.

形式上, 我们用

$$x'+px''+\cdots+p^{e-1}x^{(e)} \tag{6.4}$$

来表示所考虑的

$$g_1(x)\equiv 0\pmod{p^l} \tag{6.5}$$

的解.

**引理 6.1** 同余方程 (6.5) 在上述意义下的解数至多为 $n$.

**证明** 设 $x'$ 是 (6.1) 的 $m$ 重根, 我们只要证明 (6.3) 至多有 $m$ 个解 (按重数计). 事实上, 设 $x'_1, x'_2, \cdots, x'_v$ 是 (6.1) 的解, 相应的重数是 $m_1, m_2, \cdots, m_v$. 这样, 就相应地有 $v$ 个 $g_2(x)$, 这 $v$ 个方程 (6.3) 的总的解数 $\leqslant m_1 + \cdots + m_v \leqslant n$.

可以假定 $x' = 0$. 按定义我们可记

$$p^{-r_0} g_1(x) = x^m h(x) + pj(x),$$

这里 $j(x)$ 是次数小于 $m$ 的多项式, 及 $p \nmid h(0)$. 因而有

$$g_2(x) = p^m x^m h(px) + pj(px).$$

这也就证明了 $r_1 \leqslant m$ 及

$$\begin{aligned} p^{-r_1} g_2(x) =& p^{m-r_1} x^m h(px) + p^{1-r_1} j(px) \\ \equiv& p^{m-r_1} x^m h(0) + p^{1-r_1} j(px) (\bmod p), \end{aligned}$$

这是一个次数 $\leqslant m$ 的多项式.

## 7. 多项式的特征指数链

设

$$f(x) = a_k x^k + \cdots + a_1 x + a_0$$

及 $p \nmid (a_k, \cdots, a_1)$. 再设

$$x = x' + px'' + \cdots + p^{e-1} x^{(e)} \tag{7.1}$$

是

$$f'(x) \equiv 0 (\bmod p^l) \tag{7.2}$$

在 §6 意义下的一个解.

设 $u_1$ 是最大整数使得 $p^{u_1}$ 整除以下多项式的所有系数:

$$f(px + x') - f(x') \quad (= p^{u_1} f_1(x)).$$

再设 $u_2$ 是最大整数使得 $p^{u_2}$ 整除以下多项式的所有系数:

$$f_1(px + x'') - f_1(x'') \quad (= p^{u_2} f_2(x)).$$

因为

$$f_1(px+x'')-f_1(x'')=p^{-u_1}(f(p^2x+px''+x')-f(px''+x')),$$

所以 $p^{u_1+u_2}$ 是整除以下多项式的所有系数的 $p$ 的最高次幂:

$$f(p^2x+x'+px'')-f(x'+px'').$$

类似地, 我们定义 $u_1,u_2,\cdots$, 直至 $u_e$, 它称为是关于多项式 $f'(x)\bmod p^l$ 的解 (7.1) 的特征指数链.

**引理 7.1** 我们有

$$k\geqslant u_1\geqslant u_2\geqslant\cdots\geqslant u_e\geqslant 2. \tag{7.3}$$

**证明** 按定义显有 $u_i\geqslant 2$. 只需要证明 $k\geqslant u_1\geqslant u_2$. 无妨一般可假定 $x'=x''=0$. 因此

$$f(px)-f(0)=a_kp^kx^k+\cdots+a_1px.$$

显有 $u_1\leqslant k$, 因为 $p\nmid(a_k,\cdots,a_1)$. 从 $u_1$ 的定义知

$$p^{u_1-1}|a_1,p^{u_1-2}|a_2,\cdots,p|a_{u_1-1}. \tag{7.4}$$

若 $u_2>u_1$, 则由 $u_2$ 的定义, 即 $p^{u_1+u_2}$ 整除 $f(p^2x)-f(0)$ 的所有系数, 推出

$$p^{u_1+u_2-2}|a_1,p^{u_1+u_2-4}|a_2,\cdots,p^{u_1+u_2-2u_1}|a_{u_1}.$$

因而有

$$p^{u_1}|a_1,p^{u_1-1}|a_2,\cdots,p^2|a_{u_1-1},p|a_{u_1},$$

这意味着 $p^{u_1+1}$ 整除 $f(px)-f(0)$ 的所有系数, 这和 $u_1$ 的定义矛盾.

**引理 7.2** 我们有

$$l+e-(u_1+\cdots+u_e)\leqslant\left[\frac{\log k}{\log p}\right].$$

**证明** 无妨一般可设

$$x'+x''p+\cdots+x^{(e)}p^{e-1}=0.$$

这样, 由定义推出 $f'(p^ex)$ 的所有系数被 $p^l$ 整除, 即

$$p^l|\nu a_\nu p^{e(\nu-1)},\quad \nu=1,2,\cdots,k.$$

亦即

$$\frac{p^{l+e}}{(p^l,\nu)}\bigg|a_\nu p^{e\nu},$$

$f(p^e x)-f(0)$ 的所有系数被 $p^{l+e-\nu}$ 整除, 这里 $p^\nu=\max\limits_{1\leqslant v\leqslant k}(p^l,v)$. 所以

$$u_1+\cdots+u_e\geqslant l+e-\left[\frac{\log k}{\log p}\right],$$

因为 $(p^l,v)\leqslant p^\nu\leqslant k$.

**引理 7.3** 设 $e'\leqslant e$. 那么, 存在具有给定的前 $e'$ 个特征指数组:

$$h\geqslant u_1\geqslant u_2\geqslant\cdots\geqslant u_{e'}>1$$

的根的多项式的个数等于

$$p^{e'}p^{lk-\frac{1}{2}u_1(u_1-1)-\cdots-\frac{1}{2}u_{e'}(u_{e'}-1)}.$$

**证明** 这样的根的可能选取的个数是 $p^{e'}$. 假定这根是 0, 然后依次应用式 (7.4) 就得到引理, 因为条件 (7.4) 以因子

$$p^{-1-2-\cdots-(u_1-1)}=p^{-\frac{1}{2}u_1(u_1-1)}$$

限制了 $a_1,\cdots,a_k$ 取值的可能性.

# 8. 指 数 和

设 $p\nmid(a_k,\cdots,a_1)$ 及

$$f(x)=a_kx^k+\cdots+a_1x+a_0,$$

再设

$$W=\left[\frac{\log k}{\log p}\right].$$

设 $r$ 是最大的整数使得 $p^r$ 整除 $f'(x)$ 的所有系数. 显有 $r\leqslant W$.

**引理 8.1** 若 $\xi$ 不是

$$p^{-r}f'(x)\equiv 0(\bmod p)\tag{8.1}$$

的解, 那么当 $l>2W+1$ 时, 我们有

$$\sum_{x=1}^{p^{l-1}}e(f(\xi+px)/p^l)=0.$$

**证明** 设 $x=y+p^{l-r-2}z$, 我们有

$$\begin{aligned}&\sum_{x=1}^{p^{l-1}}e(f(\xi+px)/p^l)\\ =&\sum_{y=1}^{p^{l-r-2}}\sum_{z=0}^{p^{r+1}-1}e(f(\xi+py+p^{l-r-1}z)/p^l)\\ =&\sum_{y=1}^{p^{l-r-2}}e(f(\xi+py)/p^l)\sum_{z=0}^{p^{r+1}-1}e(f'(\xi+py)z/p^{r+1})\\ =&0,\end{aligned}$$

因为 $p^{r+1}\nmid f'(\xi)$.

**引理 8.2** 设 $\xi$ 是 (8.1) 的解, 以及 $p^{u_1}$ 是整除 $f(px+\xi)-f(\xi)(=p^{u_1}g(x))$ 的所有系数的 $p$ 的最高方幂. 那么, 我们有

$$\sum_{x=1}^{p^{l-1}}e(f(\xi+px)/p^l)=p^{u_1-1}e(f(\xi)/p^l)\sum_{x=1}^{p^{l-u_1}}e(g(x)/p^{l-u_1}). \tag{8.2}$$

**证明** 我们有

$$\begin{aligned}&\sum_{x=1}^{p^{l-1}}e((f(\xi+px)-f(\xi))/p^l)\\ =&\sum_{x=1}^{p^{l-1}}e(g(x)/p^{l-u_1})=p^{u_1-1}\sum_{x=1}^{p^{l-u_1}}e(g(x)/p^{l-u_1}).\end{aligned}$$

由引理 8.1 和 8.2 知

$$\sum_{x=1}^{p^l}e(f(x)/p^l)=\sum_{\xi}p^{u_1-1}e(f(\xi)/p^l)\sum_{x=1}^{p^{l-u_1}}e(g(x)/p^{l-u_1}),$$

其中 $\xi$ 遍历 (8.1) 的所有的根, 以及 $u_1$ 和 $g$ 与 $\xi$ 有关.

如果重复利用这个方法, 这指数和就被分解为至多 $k-l$ 个部分和, 其中的每一个在 §6 所说的意义下对应于一个根. 当然, 应该注意到 $l>2W+1$.

设 $e'$ 是最大整数, 满足

$$l-u_1-\cdots-u_{e'-1}>2W+1\geqslant l-u_1-\cdots-u_{e'}.$$

引理 7.2 保证了 $e'$ 的存在性. 以 $\xi=x'+px''+\cdots+p^{e'-1}x^{(e')}$ 表示这些根的一个代表. 那么对应于这个根的部分和等于

$$\mathrm{e}^{2\pi\mathrm{i}f(\xi)/p^l}p^{u_1}+\cdots+u_{e'-e'}\sum_{x=1}^{p^{l_0}}\mathrm{e}^{2\pi\mathrm{i}h(x)/p^{l_0}}, \tag{8.3}$$

其中

$$l_0 = l - u_1 - \cdots - u_{e'}, \quad 0 \leqslant l_0 \leqslant 2W + 1.$$

因此, 对应于具有链 $(u_1, \cdots, u_{e'})$ 的这些根中的一个部分和的绝对值是

$$\leqslant p^{u_1+\cdots+u_{e'}-e'} \cdot p^{l_0} = p^{l-e'}. \tag{8.4}$$

设

$$A(p^l) = \sum_{\substack{a_k=1 \\ p\nmid(a_k,\cdots,a_1)}}^{p^l} \cdots \sum_{a_1=1}^{p_l} \left| \frac{1}{p^l} \sum_{x=1}^{p^l} e((a_k x^k + \cdots + a_1 x)/p^l) \right|^{2t}.$$

把内层和 $\sum\limits_{x=1}^{p^l}$ 按照 $f'(x) \equiv o(\bmod p^l)$ 的根 (在 §6—§7 的意义下) 分为

$$\sum\nolimits_1, \cdots, \sum\nolimits_m, \quad m \leqslant k-1.$$

利用 Hölder 不等式, 得到

$$\left| \sum_{x=1}^{p^l} e((a_k x^k + \cdots + a_1 x)/p^l) \right|^{2t} \leqslant k^{2t-1} \sum_{i=1}^{m} \left| \sum\nolimits_i \right|^{2t}.$$

因此, $A(p^l)$ 不超过和

$$p^{-2tl} \sum_{\xi} |S(\xi)|^{2t}, \tag{8.5}$$

其中 $S(\xi)$ 对应于一个部分和, 这个部分和相应于以 $\xi$ 为根的一个多项式. 对应于一个给定的链

$$u_1, u_2, \cdots, u_{e'},$$

多项式的个数是

$$\leqslant p^{e'} \cdot p^{lk-\frac{1}{2}u_1(u_1-1)-\cdots-\frac{1}{2}u_{e'}(u_{e'}-1)},$$

以及由式 (8.4) 知每个和是

$$\leqslant p^{l-e'}.$$

因此, 所有那些部分和 (它们中的每一个对应于具有链 $u_1, \cdots, u_{e'}$ 的一个根) 的和是

$$\leqslant p^{e'+lk-\frac{1}{2}u_1(u_1-1)-\cdots-\frac{1}{2}u_{e'}(u_{e'}-1)} \cdot p^{-2e't}.$$

对 $u_1, \cdots, u_{e'}$. 所有可能的值求和, 得到

$$A(p^l) = O\left( \sum p^{e'+lk-\frac{1}{2}u_1(u_1-1)-\cdots-\frac{1}{2}u_{e'}(u_{e'}-1)-2e't} \right), \tag{8.6}$$

其中求和范围是

$$k \geqslant u_1 \geqslant u_2 \geqslant \cdots \geqslant u'_e \geqslant 2,$$

及

$$2W+1 \geqslant l-u_1-\cdots-u'_e \geqslant 0.$$

式 (8.6) 的右边的项数是 $O(l^k)$. 事实上, 我们考虑

$$u_1+\cdots+u'_e=l' \tag{8.7}$$

的解数. 假设在 $u_1,\cdots,u'_e$ 中有 $e_k$ 个等于 $k, e_{k-1}$ 个等于 $k-1,\cdots$, 及 $e_2$ 个等于 2. 那么

$$0 \leqslant ke_k \leqslant l', 0 \leqslant (k-1)e_{k-1} \leqslant l', \cdots, 0 \leqslant 2e_2 \leqslant l'.$$

因而有

$$\leqslant \frac{(l'+1)^{k-1}}{k!}=O(l'^{k-1})$$

组不同的 $u_1,\cdots,u_{e'}$ 满足 (8.7). 对 $l'=l-2W-1,\cdots,l$ 求和就得到所要的结论.

现在我们来求在式 (8.6) 中具有最高指数的项. 对给定的 $e'$, 我们来证明:

$$u_l=\cdots=u_{l'-[\frac{l'}{e'}]e'}=\left[\frac{l'}{e'}\right]+1, \quad u_{l'-[\frac{l'}{e'}]e'+1}=\cdots=u_{e'}=\left[\frac{l'}{e'}\right] \tag{8.8}$$

给出了式 (8.6) 中具有最大指数的项. 这是下述不等式的一个推论: 若 $u>\nu+1$, 则

$$\frac{u(u-1)}{2}+\frac{\nu(\nu-1)}{2}>\frac{(u-1)(u-2)}{2}+\frac{\nu(\nu+1)}{2},$$

即若指数中的两项所相应的 $u$ 和 $v$ 之差 $\geqslant 2$, 那么可分别以 $u-1$ 和 $v+1$ 来代替, 且这样得到的项给出了一个更大的指数.

在情形 (8.8), 这个指数是

$$\begin{aligned}
& e'+l'k-\frac{1}{2}\left(\left[\frac{l'}{e'}\right]+1\right)\left[\frac{l'}{e'}\right]\left(l'-\left[\frac{l'}{e'}\right]e'\right) \\
& -\frac{1}{2}\left[\frac{l'}{e'}\right]\left(\left[\frac{l'}{e'}\right]-1\right)\left(e'-l'+\left[\frac{l'}{e'}\right]e'\right)-2e't \\
=& e'+l'k+\frac{e'}{2}\left[\frac{l'}{e'}\right]\left(\left[\frac{l'}{e'}\right]-1\right)-\left[\frac{l'}{e'}\right]\left(l'-\left[\frac{l'}{e'}\right]e'\right)-2e't \qquad (8.9)\\
\leqslant & e'+l'k-\frac{e'}{2}\left[\frac{l'}{e'}\right]\left(\left[\frac{l'}{e'}\right]-1\right)-2e't=\phi(e'). \qquad (8.10)
\end{aligned}$$

设

$$t = \frac{1}{4}k(k+1) + 1 + \delta. \tag{8.11}$$

当 $e'|l'$ 时, 设 $l' = e'm, m \leqslant k$, 我们有

$$\begin{aligned}\phi(e') =& e' + e'mk - \frac{e'}{2}m(m-1) - 2e't \\ =& e'\left(1 + \frac{1}{2}m(2k-m+1) - 2t\right) \\ \leqslant& e'(1 + \frac{1}{2}k(k+1) - 2t) \leqslant -(1+2\delta)e' \\ =& -(1+2\delta)\frac{l'}{m} \leqslant -(1+2\delta)\frac{l'}{k}.\end{aligned} \tag{8.12}$$

在情形 $e' \nmid l'$, 设 $l' = e'm + e_1, 1 \leqslant e_1 < e', m+1 \leqslant k$, 我们有

$$\begin{aligned}\phi(e') =& e' + (e'm + e_1)k - \frac{e'}{2}m(m-1) - 2e't \\ \leqslant& e'\left(1 + \frac{1}{2}k(k+1) - 2t\right) = -(1+2\delta)e' \\ <& -(1+2\delta)\frac{l'}{m+1} \\ \leqslant& -(1+2\delta)\frac{l'}{k}.\end{aligned} \tag{8.13}$$

因而有

$$\phi(e') \leqslant -(1+2\delta)\frac{l-2W-1}{k}.$$

综合这些结论, 得到

**引理 8.3** 当 $t = \frac{1}{4}k(k+1) + 1 + \delta$ 时, 我们有

$$A(p^l) = O(l^k p^{-(1+2\delta)\frac{l-1}{k}}).$$

事实上, 若 $W \geqslant 1$, 则有

$$p^{\frac{2W+1}{k}} \leqslant p^{\frac{3W}{k}} = O(1).$$

**引理 8.4** 当 $t > \frac{1}{4}k(k+1) + 1$ 时, $p$-adic 密度 $\partial_p$ 收敛.

**证明**

$$\partial_p = \sum_{l=0}^{\infty} A(p^l) = O\left(\sum_{l=0}^{\infty} l^k p^{-(1+2\delta)\frac{l}{k}}\right) = O(1).$$

**注** 容易证明: 当 $t > \frac{1}{4}k(k+1)$ 时 $p$-adic 密度 $\partial_p$ 收敛, 以及当 $t = \frac{1}{4}k(k+1)$ 时发散.

# 9. 奇异级数的收敛性

**引理 9.1** 当 $t \geqslant \frac{1}{4}k(k+1)+1+\delta$ 时, 我们有

$$\sum_{l=k+1}^{\infty} A(p^l) = O(p^{-(1+2\delta)}).$$

**证明** 由引理 8.3 可得

$$\begin{aligned}\sum_{l=k+1}^{\infty} A(p^l) =& O\left(\sum_{l=k+1}^{\infty} l^k p^{-(l+2\delta)\frac{l-1}{k}}\right)\\ =& O\left(\sum_{m=0}^{\infty}(m+k+1)p^{-(1+2\delta)\frac{m}{k}}\cdot p^{-(1+2\delta)}\right).\end{aligned}$$

**引理 9.2** 当 $p>k, t\geqslant\left(\frac{3}{2}+\delta\right)k$ 时, 我们有

$$A(p) = O(p^{-(1+2\delta)}).$$

**证明** 由 Mordell 定理[7] 可得

$$\begin{aligned}&\sum_{a_1=1}^{p}\cdots\sum_{a_k=1}^{p}\left|\frac{1}{p}\sum_{x=1}^{p}e((a_kx^k+\cdots+a_1x)/p)\right|^{2t}\\ \leqslant& O\left(p^{(2t-2k)(1-\frac{1}{k})-2t+k}\frac{1}{p^k}\sum_{a_1=1}^{p}\cdots\sum_{a_k=1}^{p}\left|\sum_{x=1}^{p}e((a_kx^k+\cdots+a_1x)/p\right|^{2k}\right)\\ =& O(p^{2(t-k)(1-\frac{1}{k})-2t+2k})\\ =& O(p^{p^{-2(t-k)\frac{1}{k}}})\\ =& O(p^{-(1+2\delta)}).\end{aligned}$$

**引理 9.3** 当 $t=\frac{1}{4}k(k+1)+1+\delta, p>k$ 时, 我们有

$$A(p^2)+\cdots+A(p^k) = O(p^{-(1+2\delta)}).$$

**证明** 现在有 $W=0.l'$ 可能的取值是 $l$ 或 $l-1$. 由式 (8.12) 及 (8.13) 得

$$\begin{aligned}\phi(e') \leqslant& -1(1+2\delta)\frac{l'}{m} \leqslant -(1+2\delta) \qquad \text{当} e|l\\ \leqslant& -(1+2\delta)\frac{l'}{m+1} \leqslant -(1+2\delta), \quad \text{当} e\nmid l,\end{aligned}$$

因为现在分别有 $m \leqslant l'$ 或 $m+1 \leqslant l'$. 因而得到

$$A(p^2)+\cdots+A(p^k)=O(p^{-(1+2\delta)}).$$

综合引理 9.1, 9.2 和 9.3 得到

**引理 9.4** 当 $k \geqslant 3$ 时, 我们有

$$\partial_p - 1 = O(p^{-(1+2\delta)}).$$

**引理 9.5** 设 $k \geqslant 3$. 当 $t > \frac{1}{4}k(k+1)+1$ 时, 无穷乘积

$$\prod_p \partial_p$$

绝对收敛, 且

$$\mathfrak{S} = \prod_p \partial_p.$$

**注** 用类似的方法可以证明：当 $t>3$ 及 $k=2$ 时, $\mathfrak{S}$ 收敛. 但对这种情形, 我们可求出 $\mathfrak{S}$ 的精确值, 即

$$\mathfrak{S} = 2\frac{\zeta(t-2)}{\zeta(t-1)}.$$

能得到当 $k \geqslant 3$ 时的最佳可能指数是十分幸运的. 事实上当 $k=2$ 时, $A(p)$ 的贡献是这结论的最本质部分. 当 $k \geqslant 3$ 时要求出 $A(p)$ 的最佳可能的阶是十分困难的. 幸运的是, 当 $t>1$ 时, 对代替 $A(p^t)$ 的控制项我们能得到它的最佳可能估计.

## 10. 几 个 引 理

设 $\langle\xi\rangle = \min(\xi-[\xi], [\xi]+1-\xi), \{\xi\}=\xi-[\xi]$.

**引理 10.1** 设 $\tau \geqslant 1$,

$$\left|\alpha-\frac{h}{q}\right| \leqslant \frac{\tau}{q^2}, \quad (h,q)=1, \quad 0<q<p^s.$$

那么, 满足

$$\langle\alpha y\rangle \leqslant \frac{V}{q}, \quad f \leqslant y \leqslant f+N \tag{10.1}$$

的整数解 $y$ 的个数是

$$\leqslant 2(V+2\tau)(Nq^{-1}+1). \tag{10.2}$$

**证明** 只要证明:

$$\langle\alpha y\rangle \leqslant \frac{V}{q}, \quad f \leqslant y \leqslant f+q \tag{10.3}$$

的解的个数 $\leqslant 2(V+2\tau)$. 记

$$y=f+z,\quad \alpha=\frac{h}{q}+\frac{\tau\vartheta}{q^2},\quad |\vartheta|\leqslant 1.$$

我们有

$$\begin{aligned}\alpha y=&\frac{hz}{q}+\frac{\tau\vartheta z}{q^2}+\frac{hf}{q}+\frac{\tau\vartheta f}{q^2}\\ =&\frac{hz+[c]+\{c\}+\tau\vartheta z/q}{q},\quad |\tau\vartheta z/q|\leqslant\tau,\end{aligned}$$

其中

$$c=hf+\tau\vartheta f/q.$$

当 $q\leqslant 2(V+2\tau)$ 时, 结论是显然的. 当 $z$ 遍历模 $q$ 的完全剩余系时, $w=hz+[c]$ 也是这样. 因此

$$\alpha y=\frac{w+\sigma(w)}{q},$$

其中

$$-\tau\leqslant\{c\}-\tau\leqslant\sigma(w)\leqslant\{c\}+\tau<1+\tau.$$

显见, 满足

$$V+\tau\leqslant w<q-\tau-V-1 \tag{10.4}$$

的那些整数 $w$ 给出

$$\frac{V}{q}\leqslant\frac{w+\sigma(w)}{q}<1-\frac{V}{q},$$

它们不满足式 (10.3). 满足式 (10.4) 的整数 $w$ 的个数 $\geqslant q-2V-2\tau-2$. 所以, 满足式 (10.3) 的整数个数

$$\leqslant q-(q-2V-2\tau-2)=2V+2\tau+2\leqslant 2(V+2\tau).$$

**引理 10.2** 设 $Y\geqslant 1$, 及整数 $A_0,A_1,\cdots,A_{k-1}$ 满足

$$A_0=1,|A_r|\leqslant(r+1)Y^r,$$

那么, 由方程组

$$\nu_r=\sum_{s=r}^{k}\begin{pmatrix}s+1\\ r\end{pmatrix}A_{s-r}u_s \tag{10.5}$$

可推出 $(k+1)k\cdots(r+1)u_r$ 是 $\nu_k,\cdots,\nu_r$ 的整系数线性组合, 即

$$(k+1)k\cdots(r+1)u_r=\sum_{s=r}^{k}a_{rs}\nu_s, \tag{10.6}$$

此外

$$a_{rs} = O(Y^{s-r}). \tag{10.7}$$

**证明** 当 $r = k$ 时引理成立. 假设引理对 $k, (k-1), \cdots, r+1$ 都成立. 那么, 由式 (10.5) 及归纳假设得到

$$\begin{aligned}(k+1)\cdots(r+1)u_r &= (k+1)\cdots(r+2)(\nu_r - \sum_{s=r+1}^{k}\binom{s+1}{r}A_{s-r}u_s)\\ &= (k+1)\cdots(r+2)\nu_r - \sum_{s=r+1}^{k}\binom{s+1}{r}A_{s-r}\frac{s!}{(r+1)!}(k+1)\cdots(s+1)u_s\\ &= (k+1)\cdots(r+2)\nu_r - \sum_{s=r+1}^{k}\binom{s+1}{r}A_{s-r}\frac{s!}{(r+1)!}\sum_{u=s}^{k}a_{su}\nu_u.\end{aligned}$$

这样, 当 $k \geqslant u > r$ 时有

$$a_{su} = \sum_{u \geqslant s \geqslant r+1}^{k}\binom{s+1}{r}A_{s-r}\frac{s!}{(r+1)!}a_{su}$$

这显然是一个整数, 以及

$$a_{ru} = O\left(\sum_{u \geqslant s \geqslant r+1}|A_{s-r}||a_{su}|\right) = O(Y^{s-r}\cdot Y^{u-s}) = O(Y^{u-r}).$$

当 $u = r$ 时, 显有

$$a_{rr} = O(1).$$

**引理 10.3** 设 $\xi_1, \cdots, \xi_n$ 是实数. 那么, 对整数 $l_1, \cdots, l_n$ 我们有

$$\left\langle\sum_{i=1}^{n} l_i\xi_i\right\rangle \leqslant \sum_{i=1}^{n}|l_i|\langle\xi_i\rangle.$$

这引理是下述简单事实的一个推论:

$$\langle\xi_1 \pm \xi_2\rangle \leqslant \langle\xi_1\rangle + \langle\xi_2\rangle.$$

## 11. 单个和与平均值之间的桥

**引理 11.1** 设 $\alpha_k, \cdots, \alpha_1$ 是实数, 及

$$f(x) = \alpha_k x^k + \cdots + \alpha_1 x.$$

假定 $0<\delta_1<1,T$ 是任意整数, 以及

$$\int_0^1\cdots\int_0^1\left|\sum_{x=T+1}^{T+P}e(f(x))\right|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k=O(P^{2t_1-\frac{1}{2}k(k+1)+\delta_1}),\tag{11.1}$$

符号 $O$ 所含的常数可与 $t_1$ 及 $\delta_1$ 有关, 但后面将取 $t_1$ 和 $\delta_1$ 作为 $k$ 的函数.

设 $\beta_{k+1},\cdots,\beta_1$ 是实数, 及

$$F(x)=\beta_{k+1}x^{k+1}+\cdots+\beta_1x.$$

设 $r$ 是一个整数, $k+1\geqslant r\geqslant 2$, 假定

$$\left|\beta_r-\frac{h}{q}\right|\leqslant\frac{1}{q^2},\quad (h,q)=1,\quad 1\leqslant q\leqslant P^r.\tag{11.2}$$

那么, 对任意的 $T$, 我们有

$$S=\sum_{x=T+1}^{T+P}e(F(x))=O\begin{cases}(P^{1-\rho}), & \frac{1}{2}P\leqslant q\leqslant P^{r-1},\\ \left(P^{1-\rho}\left(\frac{q}{p^{r-1}}\right)^{\frac{1}{2t_1+k+1}}\right), & P^{r-1}\leqslant q\leqslant P^r,\end{cases}\tag{11.3}$$

其中

$$\rho=\frac{1-\delta_1}{2t_1+k+1}.\tag{11.4}$$

**证明**　这个重要的技巧是属于 Vinogradov 的. 对 $0<y\leqslant Y<P$, 我们记

$$S_0=\sum_{x=T+1}^{T+P}e(F(x+y)-F(y))=\sum_{x=T+1}^{T+P}e(\phi(x)),$$

其中

$$\phi(x)=Y_1x+\cdots+Y_{k+1}x^{k+1},$$

及

$$\begin{aligned}Y_j=&Y_j(y)=\frac{1}{j!}\frac{d^j}{dy^j}F(y)\\=&\binom{k+1}{j}\beta_{k+1}y^{k+1-j}+\cdots+\binom{j+1}{j}\beta_{j+1}y+\beta_j.\end{aligned}\tag{11.5}$$

显然有 $|S_0|=|S|+2\vartheta y,|\vartheta|\leqslant 1$. 因此

$$|S|\leqslant Y^{-1}\sum_{y=1}^{Y}|S_0|+Y.$$

应用 Hölder 不等式两次就得到

$$|S|^{2t_1} \leqslant 2^{2t_1-1}\Big(\big(Y^{-1}\sum_{y=1}^{Y}|S_0|\big)^{2t_1}+Y^{2t_1}\Big)$$
$$=O\Big(Y^{-1}\sum_{y=1}^{Y}|S_0|^{2t_1}+Y^{2t_1}\Big). \tag{11.6}$$

设

$$S_1=\sum_{x=T+1}^{T+P}e(\alpha_1 x+\cdots+\alpha_k x^k+\beta_{k+1}x^{k+1}).$$

对固定的 $y, Y_1, \cdots, Y_k$ 也随之固定; 我们考虑那些满足

$$\{\alpha_1-Y_1\}\leqslant\frac{1}{2}P^{-2}Y,\cdots,\{\alpha_k-Y_k\}\leqslant\frac{1}{2}P^{-k-1}Y,\quad 0\leqslant\alpha_i<1$$

的 $\alpha_1,\cdots,\alpha_k$. 以 $\Omega(y)$ 表示由这样的 $(\alpha_1,\cdots,\alpha_k)$ 所构成的区域. 若 $\alpha_1,\cdots,\alpha_k$ 属于 $\Omega(y)$, 则有

$$S_0=S_1+O(Y),$$

因而有

$$|S_0|^{2t_1}=O(|S_1|^{2t_1})+O(Y^{2t_1}). \tag{11.7}$$

结合式 (11.6) 和 (11.7), 得到

$$|S|^{2t_1}=O(|S_1|^{2t_1})+O(Y^{2t_1}),$$

在区域 $\Omega(y)$ 上对两边积分, 我们有

$$|S|^{2t_1}=O\Big(P^{\frac{1}{2}k(k+1)+k}Y^{-k}\int\cdots\int_{\Omega(Y)}|S_1|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\Big)+O(Y^{2t_1}), \tag{11.8}$$

因为

$$\int\cdots\int_{\Omega(y)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\geqslant\prod_{i=1}^{k}\Big(\frac{1}{2}P^{-(i+1)}Y\Big)=P^{-\frac{1}{2}k(k+1)-k}Y^k.$$

现在我们来估计重叠的 $\Omega(y)$ 的个数. 假定 $\Omega(y)$ 和 $\Omega(y_0)$ 是重叠的. 那么有

$$\langle Y_r(y)-Y_r(y_0)\rangle\leqslant P^{-r-1}Y,\quad 1\leqslant r\leqslant k.$$

令 $v_r=Y_r(y)-Y_r(y_0), u_j=\beta_{s+1}(y-y_0)$, 及

$$A_{s-r}=\frac{y^{s-r+1}-y_0^{s-r+1}}{y-y_0},$$

那么从 (11.15) 推得

$$v_r=\sum_{s=r}^{k}\binom{s+1}{r}\beta_{s+1}(y^{s-r+1}-y_0^{s-r+1})=\sum_{s=r}^{k}\binom{s+1}{r}A_{s-r}u_s.$$

利用引理 10.2 和 10.3, 我们有

$$\begin{aligned}\left\langle\frac{(k+1)!}{r!}u_r\right\rangle&\leqslant\sum_{s=r}^{k}|a_{rs}|\langle v_s\rangle=O\left(\sum_{s=r}^{k}Y^{s-r}P^{-s-1}Y\right)\\&=O(YP^{-r-1}),\qquad 1\leqslant r\leqslant k.\end{aligned}$$

以 $r-1$ 代 $r$ 得到

$$\left\langle\frac{(k+1)!}{(r-1)!}\beta_r(y-y_0)\right\rangle=O(YP^{-r}),\quad 2\leqslant r\leqslant k+1,\tag{11.9}$$

其中

$$1\leqslant y\leqslant Y.\tag{11.10}$$

由引理 10.1 知, 满足式 (11.9) 和 (11.10) 的整数 $y$ 的个数是

$$O\left(\left(\frac{Yq}{P^r}+1\right)\left(1+\frac{Y}{q}\right)\right)=O\left(\frac{qY}{P^r}+1\right)=O\left(\frac{q}{P^{r-1}}+1\right),\tag{11.11}$$

因为

$$q\geqslant\frac{1}{2}P \text{ 和 } Y\leqslant P.$$

所以在单位超立方体:

$$0\leqslant\alpha_1\leqslant 1,\cdots,0\leqslant\alpha_k\leqslant 1$$

(把它称为 $k$ 维环面更好, 即把边 $\alpha_i=0$ 和 $\alpha_i=1$ 看作是同一的) 中的任意一点 $(\alpha_1,\cdots,\alpha_k)$ 至多被 $\Omega(y),y=1,\cdots,Y$ 覆盖 $O\left(\frac{Yq}{P^r}+1\right)$ 次. 因此由式 (11.8) 可得

$$\begin{aligned}|S|^{2t_1}=&O\left(P^{\frac{1}{2}k(k+1)+k}Y^{-k}\frac{1}{Y}\sum_{y=1}^{Y}\int\cdots\int_{\Omega}|S_1|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\right)+O(Y^{2t_1})\\=&O(P^{\frac{1}{2}k(k+1)+k}Y^{-k-1}(\frac{q}{P^{r-1}}+1)\int_0^1\cdots\int_0^1|S_1|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k)+O(Y^{2t_1}).\end{aligned}\tag{11.12}$$

因为

$$\int_0^1\cdots\int_0^1\left|S_1\right|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\leqslant\int_0^1\cdots\int_0^1\left|\sum_{x=T+1}^{P+T}\mathrm{e}(f(x))\right|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k,$$

由式 (11.1) 得到

$$\begin{aligned}|S|^{2t_1} =&O\left(P^{\frac{1}{2}k(k+1)+k}Y^{-k-1}\left(\frac{q}{P^{r-1}}+1\right)P^{2t_1-\frac{1}{2}k(k+1)+\delta_1}\right)+O(Y^{2t_1})\\ =&O\left(P^{2t_1+k+\delta_1}Y^{-k-1}\left(\frac{q}{p^{r-1}}+1\right)\right)+O(Y^{2t_1}).\end{aligned}$$

取

$$Y=\begin{cases}[P^{1-\frac{1-\delta_1}{2t_1+k+1}}]+1, & \dfrac{P}{2}\leqslant q\leqslant P^{r-1},\\ \left[P^{1-\frac{1-\delta_1}{2t_1+k+1}}\left(\dfrac{q}{P^{r-1}}\right)^{\frac{1}{2t_1+k+1}}\right]+1, & P^{r-1}\leqslant q\leqslant P^r,\end{cases}$$

就推得引理.

**引理 11.2** 在引理 11.1 的相同假设下, 我们有

$$S=\sum_{x=T+1}^{T+P}e(F(x))=O(Pq^{-\rho}),\quad 1\leqslant q\leqslant P.$$

**证明** 把这个和式分为不超过 $\dfrac{P}{q}$ 部分, 每一部分是一个长度为 $Q$ 的和, $Q$ 满足

$$q\leqslant Q\leqslant 2q.$$

由引理 11.1 可得

$$\begin{aligned}S=&O\left(\frac{P}{q}\max_f\left|\sum_{x=f+1}^{f+Q}e(F(x))\right|\right)\\ =&O\left(\frac{P}{q}Q^{1-1/\rho}\right)=O(Pq^{-1/\rho}).\end{aligned}$$

# 12. 指数和估计

**引理 12.1**[1] 设

$$f(x)=\alpha_kx^k+\cdots+\alpha_1x.$$

再设 $t_1=t_1(k)$ 是由下表所定义的整数:

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $t_1$ | 1 | 3 | 8 | 23 | 62 | 380 | 656 | 889 | 2034 | 4595 |

我们有

$$\int_0^1\cdots\int_0^1\left|\sum_{x=1}^{P}\mathrm{e}^{2\pi\mathrm{i}f(x)}\right|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k=O(P^{2t_1-\frac{1}{2}k(k+1)+\varepsilon}).$$

**引理 12.2**[2]　在引理 12.1 的同样的假定下, 我们有

$$\int_0^1 \cdots \int_0^1 \left|\sum_{x=0}^{P} \mathrm{e}^{2\pi \mathrm{i} f(x)}\right|^{2t_1} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k = O(P^{2t_1 - \frac{1}{2}k(k+1)+\delta+\varepsilon}),$$

其中

$$t_1(k) = t_1 = \begin{cases} \frac{1}{4}k(k+1) + lk, & k \equiv 0, 3(\operatorname{mod} 4), \\ \frac{1}{4}(k^2 + k + 2) + lk, & k \equiv 1, 2(\operatorname{mod} 4), \end{cases}$$

以及

$$\delta(k) = \delta = \frac{1}{2}k(k+1)\left(1 - \frac{1}{k}\right)^l, \quad l \geqslant k.$$

综合这两个结论和引理 11.1, 就得到

**引理 12.3**　设 $\sigma_k$ 是由下表所定义的数:

| $k$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | $>11$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\sigma_k$ | 4 | 9 | 20 | 51 | 130 | 319 | 768 | 1781 | 4078 | 9201 | $2k^2(2\log k + \log\log k + 3)$ |

设 $k \geqslant r \geqslant 2$, 及

$$\left|\alpha_r - \frac{h}{q}\right| \leqslant \frac{1}{q^2}, \quad (h, q) = 1, \quad 1 \leqslant q \leqslant p^r; \tag{12.1}$$

再设

$$f(x) = \alpha_k x^k + \cdots + \alpha_1 x.$$

那么, 我们有

$$\sum_{x=1}^{P} e(f(x)) = O(P^{1-\frac{1}{\sigma_k}+\varepsilon}), \quad P \leqslant q \leqslant P^{r-1} \tag{12.3}$$

$$= O(Pq^{-\frac{1}{\sigma_k}+\varepsilon}), \quad 1 \leqslant q \leqslant P. \tag{12.3}$$

**证明**　当 $k \leqslant 11$ 时, 这是引理 11.1,11.2 及 12.1 的直接推论, 这里取 $\delta_1 = \varepsilon$ 及

$$\sigma_k = 2t_1 + k + 1.$$

当 $k > 11$ 时, 我们利用引理 11.1, 取

$$\delta_1 = \delta(k-1),$$

定义见引理 12.2. 这样, 由引理 12.2 得到

$$\frac{1}{\rho} = (2t_1(k-1) + k) \Big/ \left(1 - \frac{1}{2}k(k-1)\left(1 - \frac{1}{k-1}\right)^l\right)$$

$$\leqslant\left(\frac{1}{2}k^2+2lk\right)\bigg/\left(1-\frac{1}{2}k(k-1)\left(1-\frac{1}{k-1}\right)^l\right)$$
$$\leqslant\left(\frac{1}{2}k^2+2lk\right)\left(1+k^2\left(1-\frac{1}{k}\right)^l\right),\tag{12.4}$$

若

$$\frac{1}{2}k(k-1)\left(1-\frac{1}{k-1}\right)^l\leqslant\frac{1}{2},\tag{12.5}$$

因为, 当 $0\leqslant x\leqslant\frac{1}{2}$ 时, $(1-x)^{-1}\leqslant 1+2x$. 取

$$l=\left[\frac{2\log k+\log\log k}{-\log\left(1-\frac{1}{k}\right)}\right]+1,$$

则有

$$l<k(2\log k+\log\log k)+1$$

及

$$k^2\left(1-\frac{1}{k}\right)^l\leqslant\frac{1}{\log k},\tag{12.6}$$

因为

$$\frac{1}{-\log\left(1-\frac{1}{k}\right)}=\left(\frac{1}{k}+\frac{1}{2k^2}+\frac{1}{3k^3}+\cdots\right)^{-1}\leqslant k.$$

所以, 当 $k>11$ 时,

$$\frac{1}{\rho}\leqslant\left(\frac{1}{2}k^2+2k^2(2\log k+\log\log k)+2k\right)\left(1+\frac{1}{\log k}\right)$$
$$\leqslant 2k^2\left(2\log k+\log\log k+\frac{1}{4}+\frac{1}{k}+\frac{\log\log k}{\log k}+\frac{1}{4\log k}+\frac{1}{k\log k}\right)$$
$$\leqslant 2k^2(2\log k+\log\log k+3)(=\sigma_k).$$

由式 (12.6) 知, 式 (12.5) 确实成立, 所以我们就证明了式 (12.2)、(12.3) 是引理 11.2 的推论.

引理 11.1 的另一个推论是

**引理 12.4** 在引理 12.3 的相同条件下, 以及 $k\leqslant 11$, 我们有

$$\sum_{x=1}^{P}e(f(x))=O\left(P^{1-\frac{1}{\sigma_k}+\varepsilon}\left(\frac{q}{P^{r-1}}\right)^{\frac{1}{\sigma_k}}\right),\quad P^{r-1}\leqslant q\leqslant P^r.\tag{12.7}$$

当 $k > 11$ 时, 目前我们还不能得到如此精确的结果. 我们给出下面的部分结果, 它将在以后用到.

**引理 12.5** 在引理 12.3 相同条件下, 以及 $k > 11$, 我们有

$$\sum_{x=1}^{P} e(f(x)) = O(P^{1-\frac{1}{\rho'}}), \quad P^{r-1} \leqslant q \leqslant P^{r-\frac{1}{4k}}, \tag{12.8}$$

这里

$$\rho' = 40k^3\log k.$$

**证明** 由引理 11.1 可得

$$\sum_{x=1}^{P} e(f(x)) = O(P^{1-\rho}(P^{1-\frac{1}{4k}})^{\frac{1}{2t_1+k+1}}) = O(P^{1-\frac{\frac{1}{4k}-\delta_1}{2t_1+k+1}}).$$

取 $\delta_1 = \delta(k-1)$, 及

$$l = \left[\frac{4\log k}{-\log\left(1-\dfrac{1}{k}\right)}\right] + 1,$$

就有

$$l \leqslant 4k\log k + 1,$$

及

$$\delta_1 \leqslant k^2\left(1-\frac{1}{k}\right)^l \leqslant \frac{1}{k^2}.$$

如同不等式 (12.4) 一样, 我们有

$$\begin{aligned}
&(2t_1(k-1)+k+1)\Big/\left(\frac{1}{4k}-\delta_1\right)\\
\leqslant&\left(\frac{1}{2}k^2+2lk\right)\Big/\left(\frac{1}{4k}-\frac{1}{k^2}\right)\\
\leqslant&\left(\frac{1}{2}k^2+8k^2\log k+2k\right)4k\left(1-\frac{4}{k}\right)^{-1}\\
\leqslant&40k^3\log k.
\end{aligned}$$

**注** 由于下面将得到更好的结果, 所以我们不再充分利用我们的方法了.

## 13. 关于指数和估计的几个注记

前面的指数和估计都依赖于多项式的单个系数 $a_r (2 \leqslant r \leqslant k)$ 的算术性状. 看起来很象是一个满意的结果应该是依赖于系数 $\alpha_k, \cdots, \alpha_2$ 全体的算术性状. 这样的观点由下面的结论 (引理 13.2 及 13.3) 所支持.

**引理 13.1** 我们以 $\langle\xi\rangle$ 表示它到离它最近整数的距离. 设 $V_1,\cdots,V_k$ 是整数, 及 $(h_i,q_i)=1, 1\leqslant i\leqslant k$. 那么, 不等式组

$$\left\langle\frac{xh_i}{q_i}\right\rangle\leqslant\frac{V_i}{q_i},\quad 1\leqslant i\leqslant k,\quad f<x\leqslant f+N \tag{13.1}$$

的解 $x$ 的个数 $\leqslant\left(\frac{N}{Q}+1\right)\prod_{i=1}^{k}\min(2V_i+1,q_i)$, 其中 $Q$ 是 $q_1,\cdots,q_k$ 的最小公倍数.

**证明** 引理是下述命题的显然推论: 不等式组

$$\left\langle\frac{xh_i}{q_i}\right\rangle\leqslant\frac{V_i}{q_i},\quad 1\leqslant i\leqslant k,\quad f<x\leqslant f+Q$$

的解 $x$ 的个数 $T\leqslant\prod_{i=1}^{k}\min(2V_i+1,q_i)$. 由于这里 $x$ 和 $x-f$ 同时遍历模 $Q$ 的完全剩余系, 所以无妨一般可假定 $f=0$. 进而定义整数 $y$ 为

$$y\equiv xh_i(\operatorname{mod}q_i),\quad 1\leqslant i\leqslant k,$$

它是模 $Q$ 唯一确定的. 还显见, 当 $x$ 遍历模 $Q$ 的完全剩余系时 $y$ 亦是如此. 因此 $T$ 等于不等式组

$$\left\langle\frac{y}{q_i}\right\rangle\leqslant\frac{V_i}{q_i},\quad 1\leqslant i\leqslant k,\quad 0<y\leqslant Q$$

的解数. 显见, 当 $q_i\geqslant 2V_i+1$ 时, 这不等式组等价于

$$y\equiv 1,\cdots,V_i;\quad q_i-V_i,\cdots,q_i(\operatorname{mod}q_i).$$

在模 $Q$ 的一个完全剩余系中, 这样的 $y$ 的个数 $\leqslant\prod_{i=1}^{k}\min(2V_i+1,q_i)$, 因为同余方程组

$$x\equiv r_1(\operatorname{mod}q_1),\quad x\equiv r_2(\operatorname{mod}q_2)$$

对 $\operatorname{mod}\frac{q_1q_2}{(q_1,q_2)}$ 的解数 $\geqslant 1$.

**引理 13.2** 设

$$f(x)=\frac{h_{k+1}}{q_{k+1}}x^{k+1}+\cdots+\frac{h_1}{q_1}x.$$

在引理 11.1 的相同假设下, 我们有

$$S=O(P^{1-\rho}), \tag{13.2}$$

只要满足

$$1\leqslant q_r\leqslant P^{r-1},\quad 2\leqslant r\leqslant k+1,\quad P\leqslant Q_1,$$

这里 $Q_1$ 是 $q_k, \cdots, q_2$ 的最小公倍数.

**证明**　我们用证引理 11.1 的相同方法. 代替式 (11.9), 我们有

$$\left\langle \frac{(k+1)!}{r!}\frac{h_{r+1}}{q_{r+1}}(y-y_0)\right\rangle \leqslant C_1 YP^{-r}, \quad 1\leqslant y\leqslant Y, \quad 1\leqslant r\leqslant k. \tag{13.3}$$

利用引理 13.1,$V_r=[C_1 q_r YP^{-r}]+1$, 可得 (13.3) 的解数是

$$\begin{aligned}&O\left(\left(\frac{Y}{Q_1}+1\right)\prod_{r=1}^{k}\min(q_r YP^{-r}+1,q_r)\right)\\ =&O\left(\left(\frac{Y}{Q_1}+1\right)\prod_{r=1}^{k}\min(q_r P^{-r+1}+1,q_r)\right)\\ =&O(1).\end{aligned}$$

由引理 11.1 中所用的同样的方法, 我们就得到 (13.2).

我们能用引理 11.2 的方法证明: 当 $Q_1\leqslant P$ 时, 有

$$S=O(PQ_1{}^{-1/\rho}), \tag{13.4}$$

但有时我们能用下面更强的结果.

**引理 13.3**　设

$$f(x)=\frac{h_k}{q_k}x^k+\cdots+\frac{h_1}{q_1}x, \quad (h_i,q_i)=1, \quad q_i\geqslant 1,$$

$Q_1$ 是 $q_k,\cdots,q_2$ 的最小公倍数, 以及 $Q$ 是 $Q_1$ 和 $q_1$ 的最小公倍数. 那么, 我们有

$$\sum_{x=1}^{P}e(f(x))-\frac{P}{Q}\sum_{x=1}^{Q}e(f(x))=O(Q\cdot Q_1{}^{-1/k+\varepsilon}). \tag{13.5}$$

**证明**　由引理 4.1 可得

$$\frac{P}{Q}\sum_{x=1}^{Q}e(f(x))=O(PQ^{-1/k+\varepsilon}),$$

所以, 只要证明: 当 $1\leqslant P\leqslant Q$ 时有

$$\sum_{x=1}^{P}e(f(x))=O(Q\cdot Q_1^{-1/k+\varepsilon}). \tag{13.6}$$

设 $Q=d\,Q_1$. 记

$$Qf(x)=g(x)=a_kx^k+\cdots+a_2x^2+a_1x.$$

容易证明

$$(a_k, \cdots, a_2) = d. \tag{13.7}$$

因为

$$\frac{1}{Q}\sum_{n=1}^{Q}\sum_{m=1}^{P} e(n(m-x)/Q) = \begin{cases} 1, & 1 \leqslant x \leqslant P, \\ 0, & P+1 \leqslant x \leqslant Q, \end{cases}$$

故有

$$\begin{aligned}\sum_{x=1}^{P} e(g(x)/Q) &= \sum_{x=1}^{Q} e(g(x)/Q)\frac{1}{Q}\sum_{n=1}^{Q}\sum_{m=1}^{P} e(n(m-x)/Q)\\ &= \frac{P}{Q}\sum_{x=1}^{Q} e(g(x)/Q) + \frac{1}{Q}\sum_{n=1}^{Q-1}\left(\sum_{m=1}^{P} e(mn/Q)\right)\sum_{x=1}^{Q} e(g(x)-nx)/Q). \end{aligned} \tag{13.8}$$

由引理 4.1 知第一项的绝对值是 $O(PQ^{-1/k+\varepsilon}) = O(QQ_1^{-1/k+\varepsilon})$ 因为

$$\left|\sum_{m=1}^{P} e(nm/Q)\right| = \left|\frac{1-e(nP/Q)}{1-e(n/Q)}\right| \leqslant \left|\frac{1}{\sin\pi n/Q}\right| \leqslant \frac{1}{\langle n/Q\rangle},$$

以及由引理 4.1 知

$$\sum_{x=1}^{Q} e((g(x)-nx)/Q) = O(QQ_1^{-1/k+\varepsilon}),$$

所以我们有

$$\begin{aligned}\sum_{x=1}^{P} e(g(x)/Q) &= O(PQ_1^{-1/k+\varepsilon}) + O\left(Q_1^{-1/k+\varepsilon}\sum_{n=1}^{Q-1}\frac{1}{\langle n/Q\rangle}\right)\\ &= O(QQ_1^{-1/k+\varepsilon}) + O\left(Q_1^{-1/k+\varepsilon}\sum_{n=1}^{1/2Q}\frac{Q}{n}\right)\\ &= O(QQ_1^{-1/k+\varepsilon}).\end{aligned}$$

这就证明了引理.

当 $Q \leqslant P$ 时有

$$\sum_{x=1}^{P} e(f(x)) = O(PQ^{-1/k}),$$

这是一个比 (13.4) 更强的结果. 对小的 $Q_1$, 这两个估计都是不好的. 下面的简单引理有时可弥补这一缺陷.

**引理 13.4**　若 $Q_1 < Q$, 则有

$$\sum_{x=1}^{P} e(f(x)) = O(Q).$$

**证明**　当 $P \leqslant Q$ 时, 引理是显然的. 假定 $Q < P$. 设 $x = Q_1 y + z$, 这里

$$1 \leqslant z \leqslant Q_1, \quad 0 \leqslant y \leqslant \frac{P-z}{Q_1}.$$

因为 $q_1 \nmid Q_1$, 故有

$$\begin{aligned}\left|\sum_{x=1}^{P} e(f(x))\right| &= \left|\sum_{z=1}^{Q_1} e(f(z)) \sum_{y=1}^{(P-z)/Q_1} \mathrm{e}^{2\pi \mathrm{i} h_1 Q_1 y/q_1}\right| \\ &\leqslant Q_1 \max_{z} \left|\sum_{y} \mathrm{e}^{2\pi \mathrm{i} h_1 Q_1 y/q_1}\right| \\ &\leqslant Q_1 \frac{1}{\langle h_1 Q_1/q_1 \rangle} \leqslant Q_1 \frac{q_1}{(Q_1, q_1)} = Q.\end{aligned}$$

## 14. 定理的解析形式

设

$$T(\alpha_1, \cdots, \alpha_k) = \sum_{x=1}^{P} e(\alpha_k x^k + \cdots + \alpha_1 x). \tag{14.1}$$

由函数系 $e(nx)$ 的正交性可得

$$r_t(P) = \int_0^1 \cdots \int_0^1 |T(\alpha_1, \cdots, \alpha_k)|^{2t} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k.$$

由函数 $T(\alpha_1, \cdots, \alpha_k)$ 的周期性知, 我们可表为

$$r_t(P) = \int_{-\frac{1}{\tau_1}}^{1-\frac{1}{\tau_1}} \cdots \int_{-\frac{1}{\tau_k}}^{1-\frac{1}{\tau_k}} |T(\alpha_1, \cdots, \alpha_k)|^{2t} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k, \tag{14.2}$$

其中

$$\tau_1 = P^{\frac{1}{2}}, \quad \tau_\nu = P^{\nu - \frac{1}{2k} + \sigma}, \quad 2 \leqslant \nu \leqslant k,$$

及

$$\sigma = \frac{1}{k^3}.$$

大家知道, 对 $k$ 维空间的每一个点 $(\alpha_1, \cdots, \alpha_k)$, 必有一个有理点 $\left(\frac{h_1}{q_1}, \cdots, \frac{h_k}{q_k}\right)$ 使得

$$\alpha_\nu = \frac{h_\nu}{q_\nu} + \beta_\nu, \quad (h_\nu, q_\nu) = 1, \quad |\beta_\nu| \leqslant \frac{1}{q_\nu \tau_\nu}, \quad 0 < q_\nu \leqslant \tau_\nu. \tag{14.3}$$

设

$$\mathfrak{M}=\mathfrak{M}\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)$$

是由 $|\beta_\nu|\leqslant\frac{1}{q_\nu\tau_\nu}(1\leqslant\nu\leqslant k)$ 所确定的区域, 并满足条件

$$1\leqslant q_\nu\leqslant P^{\frac{1}{2k}-2\sigma}\quad(2\leqslant\nu\leqslant k),\quad 1\leqslant q_1\leqslant P^{\frac{1}{2}-\frac{1}{2k}+\sigma},\tag{14.4}$$

容易证明, 这组区域中任意两个都是不相交的. 事实上, 假如

$$\mathfrak{M}\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\text{ 和 }\mathfrak{M}\left(\frac{h'_k}{q'_k},\cdots,\frac{h'_1}{q'_1}\right)$$

相交, 那么除了对所有 $\nu$ 有 $\frac{h_\nu}{q_\nu}=\frac{h'_\nu}{q'_\nu}$ 成立的情形外, 必有一个 $\nu$ 使得 $\frac{h_\nu}{q_\nu}\neq\frac{h'_\nu}{q'_\nu}$, 这时有

$$\frac{1}{q_\nu q'_\nu}\leqslant\frac{|h_\nu q'_\nu-h'_\nu q_\nu|}{q_\nu q'_\nu}=\left|\frac{h_\nu}{q_\nu}-\frac{h'_\nu}{q'_\nu}\right|\leqslant\frac{1}{q_\nu\tau_\nu}+\frac{1}{q'_\nu\tau_\nu}\leqslant\frac{2}{\tau_\nu}\max\left(\frac{1}{q_\nu},\frac{1}{q'_\nu}\right).$$

即

$$\tau_\nu\leqslant 2\max(q_\nu,q'_\nu)\begin{cases}\leqslant 2P^{\frac{1}{2k}-2\sigma}, & \nu>1,\\ \leqslant 2P^{\frac{1}{2}-\frac{1}{2k}-\sigma}, & \nu=1,\end{cases}$$

而这是不可能的.

以 $E$ 表示区间

$$-\frac{1}{\tau_\nu}\leqslant\alpha_\nu\leqslant 1-\frac{1}{\tau_\nu}$$

中除去所有这些区域 $\mathfrak{M}$ 后所剩下的部分. 我们设

$$T_{(1)}=\int\cdots\int_E|T(\alpha_1,\cdots,\alpha_k)|^{2t}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\tag{14.5}$$

及

$$T_{(2)}=\sum_{\mathfrak{M}}K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right),\tag{14.6}$$

这里

$$K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\int\cdots\int_{\mathfrak{M}}|T|^{2t}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.\tag{14.7}$$

这样就有

$$r_t(P)=T_{(1)}+T_{(2)}.\tag{14.8}$$

## 15. $T_{(1)}$ 的估计

**引理 15.1**　设 $(\alpha_1, \cdots, \alpha_k)$ 属于 $E$, 且满足 (14.3) 及

$$1 \leqslant q_\nu \leqslant P^{\frac{1}{2k}-2\sigma}, \quad 2 \leqslant \nu \leqslant k, \tag{15.1}$$

那么有

$$T(\alpha_1, \cdots, \alpha_k) = O(P^{1-\sigma}). \tag{15.2}$$

**证明**　对任意的 $n$, 由引理 13.4 可得

$$\begin{aligned} S_n =& \sum_{x=1}^{n} e\left(\frac{h_k}{q_k}x^k + \cdots + \frac{h_1}{q_1}x\right) = O(q_1 \cdots q_k) \\ =& O(P^{\frac{1}{2}}(P^{\frac{1}{2k}-2\sigma})^{k-1}) = O(P^{1-\frac{1}{2k}-2\sigma(k-1)}). \end{aligned} \tag{15.3}$$

因而有

$$\begin{aligned} T(\alpha_1, \cdots, \alpha_k) =& \sum_{x=1}^{P}(S_x - S_{x-1})e(\beta_k x^k + \cdots + \beta_1 x) \\ =& \sum_{x=1}^{P} S_x\Big(e(\beta_k x^k + \cdots + \beta_1 x) - e(\beta_k(x+1)^k + \cdots \\ & + \beta_1(x+1))\Big) + S_P e\Big(\beta_k(P+1)^k + \cdots + \beta_1(P+1)\Big). \end{aligned} \tag{15.4}$$

因为

$$\begin{aligned} & e(\beta_k x^k + \cdots + \beta_1 x) - e(\beta_k(x+1)^k + \cdots + \beta_1(x+1)) \\ =& O(|\beta_k|P^{k-1} + |\beta_{k-1}|P^{k-2} + \cdots + |\beta_1|) \\ =& O\left(\frac{P^{k-1}}{\tau_k} + \frac{P^{k-2}}{\tau_{k-1}} + \cdots + \frac{P}{\tau_2} + \frac{1}{q_1\tau_1}\right) \\ =& O(P^{-1+\frac{1}{2k}-\sigma} + P^{-\frac{1}{2}-\frac{1}{2}+\frac{1}{2k}-\sigma}) \\ =& O(P^{-1+\frac{1}{2k}-\sigma}). \end{aligned}$$

所以, 从 (14.4),(15.1) 及 $(\alpha_1, \cdots, \alpha_k)$ 属于 $E$, 就推出 $q_1 \geqslant P^{\frac{1}{2}-\frac{1}{2k}+\sigma}$. 所以, 由 (15.3) 及 (15.4) 得到

$$\begin{aligned} T(\alpha_1, \cdots, \alpha_k) =& O\left(\sum P^{1-\frac{1}{2k}-2\sigma(k-1)} \cdot P^{-1+\frac{1}{2k}-\sigma}\right) \\ =& O(P^{1-\sigma(2k-3)}) = O(P^{1-\sigma}). \end{aligned}$$

**引理 15.2** 当 $(\alpha_1,\cdots,\alpha_k)$ 属于 $E$ 时, 我们有

$$T(\alpha_1,\cdots,\alpha_k)=O(P^{1-1/\lambda}), \tag{15.5}$$

这里

$$\lambda=40k^3\log k.$$

**证明** 以下 $k$ 个条件总有一个成立:

$$P^{\frac{1}{2k}-2\sigma}<q_\nu\leqslant P^{\nu-\frac{1}{2k}+\sigma},\quad 1<\nu\leqslant k, \tag{15.6}$$

$$P^{\frac{1}{2}-\frac{1}{2k}+\sigma}<q_1\leqslant P^{\frac{1}{2}}. \tag{15.7}$$

在第一种情形, 当 $k>11$ 时, 由引理 12.3,12.4 及 12.5 得到

$$T(\alpha_1,\cdots,\alpha_k)=O(P^{1-\frac{1}{40k^3\log k}}),$$

因为当 $P^{\frac{1}{2k}-2\sigma}\leqslant q\leqslant P$ 时, 有

$$T(\alpha_1,\cdots,\alpha_k)=O(P\cdot q^{-\frac{1}{\sigma_k}+\varepsilon})=O(P^{1-\frac{1}{40k^3\log k}}).$$

对 $k\leqslant 11$, 有

$$T(\alpha_1,\cdots,\alpha_k)=O(P^{1-\frac{1}{\sigma_k}+\varepsilon}).$$

在第二种情形, 结论可由引理 15.1 推得.

**引理 15.3** 当

$$\begin{aligned}&t\geqslant k^2(3\log k+\log\log k+4), && k\geqslant 11,\\ &t>t_0, && k\leqslant 10\end{aligned}$$

时, 我们有

$$T_{(1)}=O(P^{2t-\frac{1}{2}k(k+1)-c_1}).$$

**证明** 当 $k\leqslant 10$ 时, 证明是简单的, 现假定 $k\geqslant 11$. 设 $t_1=t_1(k)$ 是由引理 12.2 所定义, 及 $t=t_1+k^2$. 那么, 由引理 12.2 得

$$\begin{aligned}\int\cdots\int_E|T|^{2t}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k&\leqslant\max_{\alpha\in E}|T|^{2k^2}\int_0^1\cdots\int_0^1|T|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ &=O(P^{2k^2(1-1/40k^3\log k)}\cdot P^{2t_1-\frac{1}{2}k(k+1)+\frac{1}{2}k(k+1)(1-1/k)^l})\\ &=O(P^{2t-\frac{1}{2}k(k+1)-\lambda}),\end{aligned}$$

其中

$$\lambda=\frac{1}{20k\log k}-\frac{1}{2}k(k+1)(1-1/k)^l.$$

我们选取

$$l = \left[\log(10k^2(k+1)\log k) \Big/ \left(-\log\left(1-\frac{1}{k}\right)\right)\right] + 1,$$

这时有 $\lambda > 0$. 因为当 $k \geqslant 11$ 时,

$$l \leqslant k\log(22k^3\log k) + 1,$$

所以有

$$\begin{aligned}
t =& t_1 + k^2 \leqslant lk + \frac{1}{4}(k^2+k+2) + k^2 \\
\leqslant& k^2(3\log k + \log\log k + \log 22) + \frac{5}{4}(k^2+k+2) \\
=& k^2\left(3\log k + \log\log k + \log 22 + \frac{5}{4}\left(1+\frac{1}{k}+\frac{2}{k^2}\right)\right) \\
\leqslant& k^2(3\log k + \log\log k + 4).
\end{aligned}$$

## 16. 渐 近 公 式

**引理 16.1**(van der Corput)　设 $f(x)$ 是定义在区间 $(a,b)$ 上的实多项式, 它的导数满足条件

$$|f'(x)| \leqslant \frac{1}{2}.$$

那么有

$$\sum_{a\leqslant x\leqslant b} e(f(x)) = \int_a^b e(f(x))\mathrm{d}x + O(1).$$

**引理 16.2**　若 $(\alpha_1,\cdots,\alpha_k)$ 属于 $\mathfrak{M}\left(\frac{h_1}{q_1},\cdots,\frac{h_k}{q_k}\right)$, 那么有

$$T(\alpha_1,\cdots,\alpha_k) = B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)R + O(H),$$

这里 (记 $H = q_1\cdots q_k$)

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right) = \frac{1}{H}\sum_{y=1}^{H} e\left(\frac{h_k}{q_k}y^k + \cdots + \frac{h_1}{q_1}y\right)$$

及

$$R = \int_0^P e(\beta_k x^k + \cdots + \beta_1 x)\mathrm{d}x.$$

**证明** 设 $H=q_1\cdots q_k$. 记

$$x=Hz+y,\quad y=1,\cdots,H;\quad -\frac{y}{H}\leqslant z\leqslant\frac{P-y}{H}.$$

这样就有

$$T(\alpha_1,\cdots,\alpha_k)=\sum_{y=1}^{H}e\left(\frac{h_k}{q_k}y^k+\cdots+\frac{h_1}{q_1}y\right)W_y,$$

其中

$$W_y=\sum_{-\frac{y}{H}\leqslant z\leqslant\frac{P-y}{H}}e(\varphi(z))$$

及

$$\varphi(z)=\beta_k(Hz+y)^k+\cdots+\beta_1(Hz+y).$$

因为

$$\begin{aligned}\varphi'(z)=&k\beta_k(Hz+y)^{k-1}H+\cdots+\beta_1H\\=&O(|\beta_k|P^{k-1}H+|\beta_{k-1}|P^{k-2}H+\cdots+|\beta_1|H)\\=&O\left(\sum_{\nu=2}^{k}\frac{HP^{\nu-1}}{q_\nu\tau_\nu}+\frac{H}{q_1\tau_1}\right)\\=&O\left(\sum_{\nu=2}^{k}P^{(\frac{1}{2k}-2\sigma)(k-2)}\cdot P^{\frac{1}{2}-\frac{1}{2k}+\sigma}\cdot\frac{P^{\nu-1}}{P^{\nu-\frac{1}{2k}+\sigma}}+P^{(\frac{1}{2k}-2\sigma)(k-1)}\cdot\frac{1}{P^{\frac{1}{2}}}\right)\\=&O(P^{-\frac{1}{k}-2\sigma(k-2)}+P^{-\frac{1}{2k}-2\sigma(k-1)})=o(1),\end{aligned}$$

当 $P$ 趋于无穷, 即当 $P$ 充分大时, $|\varphi'(z)|\leqslant\frac{1}{2}$. 由引理 16.1, 得到

$$\begin{aligned}W_y=&\int_{-\frac{y}{H}}^{(P-y)/H}e(\varphi(z))dz+O(1)\\=&\frac{1}{H}\int_0^P e(\beta_kx^k+\cdots+\beta_1x)\mathrm{d}x+O(1).\end{aligned}$$

故有

$$\begin{aligned}T(\alpha_1,\cdots,\alpha_k)=&\frac{1}{H}\sum_{y=1}^{H}e\left(\frac{h_k}{q_k}x^k+\cdots+\frac{h_1}{q_1}x\right)\\&\times\int_0^P e(\beta_kx^k+\cdots+\beta_1x)\mathrm{d}x+O(H).\end{aligned}$$

**引理 16.3** 设 $\gamma_r=\beta_rP^r(1\leqslant r\leqslant k)$, 我们有

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)R=O(PH^{-\frac{1}{k^2}+\varepsilon}Z),$$

其中

$$Z=\min(1,|\gamma_1|^{-\frac{1}{k}},\cdots,|\gamma_k|^{-\frac{1}{k}}).$$

**证明** 设 $Q$ 是 $q_1,\cdots,q_k$ 的最小公倍数. 由引理 4.1 得

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\frac{1}{Q}\sum_{y=1}^{Q}e\left(Q\left(\frac{h_k}{q_k}x^k+\cdots+\frac{h_1}{q_1}x\right)\Big/Q\right)=O(Q^{-\frac{1}{k}+\varepsilon}).$$

因为

$$Q\geqslant\max(q_1,\cdots,q_k)\geqslant(q_1\cdots q_k)^{\frac{1}{k}}=H^{\frac{1}{k}},$$

所以有

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=O(H^{-\frac{1}{k^2}+\varepsilon}).$$

进而得

$$R=P\int_0^1 e(\gamma_k x^k+\cdots+\gamma_1 x)\mathrm{d}x.$$

从引理 3.2 就推得本引理.

**引理 16.4** 在 $\mathfrak{M}$ 上, 我们有

$$T(\alpha_1,\cdots,\alpha_k)=O(PH^{-\frac{1}{k^2}+\varepsilon}Z).$$

**证明** 因为 $\alpha$ 在 $\mathfrak{M}$ 上, 所以有

$$H=q_1\cdots q_k\leqslant P^{\frac{1}{2}-\frac{1}{2k}+\sigma+(k-1)(\frac{1}{2k}-2\sigma)}=P^{1-\frac{1}{k}-(2k-3)\sigma}\leqslant P^{1-\frac{1}{k}},$$

及

$$\begin{aligned}Z=&\min(1,|\gamma_1|^{-\frac{1}{k}},\cdots,|\gamma_k|^{-\frac{1}{k}})\\=&\min(1,(P|\beta_1|)^{-\frac{1}{k}},\cdots,(P^k|\beta_k|)^{-\frac{1}{k}})\\\geqslant&\min\left(1,\left(\frac{P}{\tau_1}\right)^{-\frac{1}{k}},\cdots,\left(\frac{P^k}{\tau_k}\right)^{-\frac{1}{k}}\right)\\\geqslant&\min(1,P^{-\frac{1}{2k}})=P^{-\frac{1}{2k}}.\end{aligned}$$

所以

$$\begin{aligned}H=&H^{-\frac{1}{k^2}+\varepsilon}\cdot H^{1+\frac{1}{k^2}-\varepsilon}\\\leqslant&H^{-\frac{1}{k^2}+\varepsilon}P^{(1+\frac{1}{k^2}-\varepsilon)(1-\frac{1}{k})}\\\leqslant&H^{-\frac{1}{k^2}+\varepsilon}P\cdot P^{-\frac{1}{2k}}=O(PH^{-\frac{1}{k^2}+\varepsilon}Z).\end{aligned}$$

从引理 16.3 就推出本引理.

# 17. 主　项

**引理 17.1**　我们有

$$K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}\int_{-q_k^{-1}\tau_k^{-1}}^{q_k^{-1}\tau_k^{-1}}\cdots\int_{-q_1^{-1}\tau_1^{-1}}^{q_1^{-1}\tau_1^{-1}}|R|^{2t}\mathrm{d}\beta_1\cdots\mathrm{d}\beta_k$$
$$+O(P^{2t-\frac{1}{2}k(k+1)-1}H^{1-(2t-1)/k^2+\varepsilon}). \tag{17.1}$$

**证明**　利用不等式

$$||\xi|^{2t}-|\eta|^{2t}|\leqslant 2t|\xi-\eta|(|\xi|^{2t-1}+|\eta|^{2t-1}),$$

可得, 在 $\mathfrak{M}\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)$ 上有

$$|T(\alpha_1,\cdots,\alpha_k)|^{2t}-\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}|R|^{2t}$$
$$=O(H(PH^{-\frac{1}{k^2}+\varepsilon}Z)^{2t-1}).$$

在区域 $\mathfrak{M}\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)$ 上积分, 得到

$$K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}\int_{-q_k^{-1}\tau_k^{-1}}^{q_k^{-1}\tau_k^{-1}}\cdots\int_{-q_1^{-1}\tau_1^{-1}}^{q_1^{-1}\tau_1^{-1}}|R|^{2t}\mathrm{d}\beta_1\cdots\mathrm{d}\beta_k$$
$$+O\left(HP^{2t-1}H^{-\frac{2t-1}{k^2}+\varepsilon}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}Z^{2t-1}\mathrm{d}\beta_1\cdots\mathrm{d}\beta_k\right). \tag{17.2}$$

设 $\delta_\nu=\max(1,|\gamma_\nu|)$. 显有

$$\prod_{\nu=1}^{k}\delta_\nu=\prod_{\nu=1}^{k}\max(1,|\gamma_\nu|)\leqslant\max(1,|\gamma_1|,\cdots,|\gamma_k|)^k,$$

因而

$$Z\leqslant\prod_{\nu=1}^{k}\delta_\nu^{-\frac{1}{k^2}}. \tag{17.3}$$

所以有

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}Z^{2t-1}\mathrm{d}\beta_1\cdots\mathrm{d}\beta_k$$
$$=P^{-\frac{1}{2}k(k+1)}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}Z^{2t-1}\mathrm{d}\gamma_1\cdots\mathrm{d}\gamma_k$$

$$\leqslant P^{-\frac{1}{2}k(k+1)}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\frac{\mathrm{d}\gamma_1\cdots\mathrm{d}\gamma_k}{(\delta_1\cdots\delta_k)^{(2t-1)/k^2}}$$
$$=O(P^{-\frac{1}{2}k(k+1)}),$$

因为 $\dfrac{2t-1}{k^2}>1$(即 $2t>k^2+1$). 引理得证.

**引理 17.2** 我们有

$$P^{-2t+\frac{1}{2}k(k+1)}\int_{-q_k^{-1}\tau_k^{-1}}^{q_k^{-1}\tau_k^{-1}}\cdots\int_{-q_1^{-1}\tau_1^{-1}}^{q_1^{-1}\tau_1^{-1}}|R|^{2t}\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1=\vartheta_0+O(P^{-(\frac{2t}{k^2}-1)\sigma}). \tag{17.4}$$

**证明** 作变量替换 $\beta_\nu=P^{-\nu}\gamma_\nu$, 等式左边等于

$$\int_{-q_k^{-1}\tau_k^{-1}P^k}^{q_k^{-1}\tau_k^{-1}P^k}\cdots\int_{-q_1^{-1}\tau_1^{-1}P}^{q_1^{-1}\tau_1^{-1}P}\left|\int_0^1 e(\gamma_k x^k+\cdots+\gamma_1 x)\mathrm{d}x\right|^{2t}\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1$$
$$=\vartheta_0+O\left(\sum_{j=1}^k\int_{-\infty}^{\infty}\mathrm{d}\gamma_1\cdots\int_{-\infty}^{\infty}\mathrm{d}\gamma_{j-1}\int_{\tau_j^{-1}q_j^{-1}P^j}^{\infty}\mathrm{d}\gamma_j\int_{-\infty}^{\infty}\mathrm{d}\gamma_{j+1}\cdots\int_{-\infty}^{\infty}|Z|^{2t}\mathrm{d}\gamma_k\right)$$
$$=\vartheta_0+O\left(\sum_{j=1}^k\int_{\tau_j^{-1}q_j^{-1}P^j}^{\infty}\delta_j^{-2t/k^2}\mathrm{d}\gamma_j\right).$$

因为

$$\frac{P^j}{q_j\tau_j}\geqslant\frac{P_j}{P^{\frac{1}{2k}-2\sigma}P^{j-\frac{1}{2k}+\sigma}}=P^\sigma,\quad 2\leqslant j\leqslant k,$$

及

$$\frac{P}{q_1\tau_1}\geqslant\frac{P}{P^{\frac{1}{2}-\frac{1}{2k}+\sigma}P^{\frac{1}{2}}}=P^{\frac{1}{2k}-\sigma}\geqslant P^\sigma,$$

所以, 左边等于

$$\vartheta_0+O\left(\int_{P^\sigma}^{\infty}\delta^{-\frac{2t}{k^2}}\mathrm{d}\gamma\right)=\vartheta_0+O\left(\int_{P^\sigma}^{\infty}\gamma^{-\frac{2t}{k^2}}\mathrm{d}\gamma\right)=\vartheta_0+O(P^{-(\frac{2t}{k^2}-1)\sigma}).$$

**引理 17.3** 我们有

$$\mathfrak{S}-\sum_{q_1\leqslant P^{\frac{1}{2}-\frac{1}{2k}+\sigma}}\sum_{q_2\leqslant P^{2-\frac{1}{2k}+\sigma}}\cdots\sum_{q_k\leqslant P^{k-\frac{1}{2k}+\sigma}}\sum_{\substack{h_1=1\\(h_1,q_1)=1}}^{q_1}\cdots\sum_{\substack{h_k=1\\(h_k,q_k)=1}}^{q_k}\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}$$
$$=O(P^{-\frac{1}{k}(\frac{1}{2}-\frac{1}{2k}+\sigma)+\varepsilon}). \tag{17.5}$$

**证明** 右边不超过

$$F\sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}\sum_{h_1}\cdots\sum_{h_k}\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t-1}=O(F),$$

其中

$$F=\max_{Q\geqslant P^{\frac{1}{2}-\frac{1}{2k}+\sigma}}\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|$$

以及 $Q$ 是 $q_1,\cdots,q_k$ 的最小公倍数. 由引理 4.1 推出

$$F=O(Q^{-\frac{1}{k}\varepsilon})=O(P^{-\frac{1}{k}(\frac{1}{2}-\frac{1}{2k}+\sigma)+\varepsilon}).$$

**引理 17.4** 我们有

$$T_{(2)}\sim\vartheta_0\mathfrak{S}P^{2t-\frac{1}{2}k(k+1)}.$$

**证明** 式 (17.1) 两边对各个 $h$ 及 $q$ 求和, 得到

$$\begin{aligned}T_{(2)}=&\sum_{h,q}\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}\int_{-q_k^{-1}\tau_k^{-1}}^{q_k^{-1}\tau_k^{-1}}\cdots\int_{-q_1^{-1}\tau_1^{-1}}^{q_1^{-1}\tau_1^{-1}}|R|^{2t}\mathrm{d}\beta_1\cdots\mathrm{d}\beta_k\\&+O\left(P^{2t-\frac{1}{2}k(k+1)-1}\sum_{q,h}H^{1-\frac{2t-1}{k^2}+\varepsilon}\right).\end{aligned}\tag{17.6}$$

级数

$$\sum_{q,h}H^{1-(2t-1)/k^2+\varepsilon}=\sum_{q}H^{2-(2t-1)/k^2+\varepsilon}$$

当 $2t>3k^2+1$ 时收敛, 即当 $k\geqslant5$ 时,

$$\sum_{q,h}H^{1-(2t-1)/k^2+\varepsilon}=O(1).$$

在 $2\leqslant k\leqslant4$ 的情形, 我们可直接证明

$$\sum_{q,h}H^{1-(2t-1)/k^2+\varepsilon}=O(P^{1-c_k}),\quad c_k>0,\quad c_2=\frac{3}{8}.$$

例如 $k=2$ 时, 有

$$\begin{aligned}&\sum_{q_1\leqslant P^{\frac{1}{2}-\frac{1}{4}+\sigma}}\ \sum_{q_2\leqslant P^{\frac{1}{4}-2\sigma}}(q_1q_2)^{2-(8-1)/4+\varepsilon}\\=&\sum_{q_1\leqslant P^{\frac{1}{4}+\sigma}}q_1^{\frac{1}{4}+\varepsilon}\sum_{q_2\leqslant P^{\frac{1}{4}-2\sigma}}q_2^{\frac{1}{4}+\varepsilon}\\=&O(P^{\frac{5}{4}(\frac{1}{4}+\sigma)+\frac{5}{4}(\frac{1}{4}-2\sigma)+\varepsilon})=O(P^{\frac{5}{8}}).\end{aligned}$$

当 $k=3$ 时,

$$\sum_{q_1\leqslant P^{\frac{1}{2}-\frac{1}{6}+\sigma}}\ \sum_{q_2\leqslant P^{\frac{1}{6}-2\sigma}}\ \sum_{q_3\leqslant P^{\frac{1}{6}-2\sigma}}(q_1q_2q_3)^{2-(18-1)/9+\varepsilon}$$

$$\leqslant \sum_{q_1 \leqslant P^{\frac{1}{3}+\sigma}} q_1^{\frac{1}{9}+\varepsilon} \sum_{q_2 \leqslant P^{\frac{1}{6}-2\sigma}} q_2^{\frac{1}{9}+\varepsilon} \sum_{q_3 \leqslant P^{\frac{1}{6}-2\sigma}} q_3^{\frac{1}{9}+\varepsilon}$$

$$=O(P^{\frac{10}{9}(\frac{1}{3}+\sigma+\frac{1}{6}-2\sigma+\frac{1}{6}-2\sigma)}) = O(P^{\frac{20}{27}}).$$

当 $k=4$ 时,

$$\sum_{q_1 \leqslant P^{\frac{1}{2}-\frac{1}{8}+\sigma}} \sum_{q_2 \leqslant P^{\frac{1}{8}-2\sigma}} \sum_{q_3 \leqslant P^{\frac{1}{8}-2\sigma}} \sum_{q_4 \leqslant P^{\frac{1}{8}-2\sigma}} (q_1q_2q_3q_4)^{2-(48-1)/10+\varepsilon}$$

$$=O(P^{\frac{1}{16}(\frac{3}{8}+\frac{3}{8})}) = O(P^{\frac{3}{64}}).$$

所以, 式 (17.6) 中的误差项可代之以

$$O(P^{2t-\frac{1}{2}k(k+1)-\frac{3}{8}}).$$

利用引理 17.2 和 17.3, 就得到

$$T_{(2)} = \sum_{h,q} \left| B\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)\right|^{2t} \vartheta_0 P^{2t-\frac{k}{2}(k+1)}$$

$$+ O(P^{2t-\frac{1}{2}k(k+1)-(2t/k^2-1)\sigma}) + O(P^{2t-\frac{1}{2}k(k+1)-\frac{3}{8}})$$

$$=\mathfrak{S}(P)\vartheta_0 P^{2t-\frac{1}{2}k(k+1)} + O(P^{2t-\frac{1}{2}k(k+1)-c_1}).$$

**式 (1.3) 的证明** 结合引理 15.3 和 17.4, 就证明了以式 (1.3) 表述的定理.

## 18. 指数和估计

现在, 我们来回答 §12 结束时所提出的问题. 代替引理 12.5, 我们将得到下面更为满意的结果.

**引理 18.1** 在引理 12.5 相同的假设下, 当 $k \geqslant 11$ 时, 有

$$\sum_{x=1}^{p} e(f(x)) = O\left(P^{1-\frac{1}{\sigma'}}\left(\frac{q}{P^{r-1}}\right)^{\frac{1}{\sigma'}}\right), \quad P^{r-1} \leqslant q \leqslant P^r,$$

其中

$$\sigma' = k^2(3\log k + \log\log k + 5).$$

这是引理 11.1($\delta = 0$) 的直接推论.

# 19. 关于 Prouhet 问题的一点注记

设 $r_t^{(l)}(P)$ 是下述具有 $l$ 组未知数 $x_1,\cdots,x_t;y_1,\cdots,y_t;\cdots,\omega_1,\cdots,\omega_t$ 的不定方程组的解数:

$$\begin{cases} x_1^k+\cdots+x_t^k=y_1^k+\cdots+y_t^k=\cdots=\omega_1^k+\cdots+\omega_t^k, \\ x_1^{k-1}+\cdots+x_t^{k-1}=y_1^{k-1}+\cdots+y_t^{k-1}=\cdots \\ \qquad\qquad =\omega_1^{k-1}+\cdots+\omega_t^{k-1}, \\ \qquad\qquad \cdots\cdots \\ x_1+\cdots+x_t=y_1+\cdots+y_t=\cdots=\omega_1+\cdots+\omega_t, \end{cases} \tag{19.1}$$

并满足条件

$$1\leqslant x_i,y_i,\cdots,\omega_i\leqslant P,\quad i=1,2,\cdots,t. \tag{19.2}$$

特别的, 我们有

$$r_t^{(2)}(P)=r_t(P).$$

下面是 $r_t^{(l)}(P)$ 的分析表达式:
设

$$T(\alpha)=\sum_{x=1}^{P}e(\alpha_kx^k+\cdots+\alpha_1x).$$

我们有

$$\begin{aligned} r_t^{(l)}(P)=\int_0^1\cdots\int_0^1&\{T_P(\alpha^{(1)})T_P(\alpha^{(2)})\cdots T_P(\alpha^{(l)})\}^t \\ &\times\tau(-\alpha^{(1)}-\cdots-\alpha^{(l)})\mathrm{d}\alpha^{(1)}\cdots\mathrm{d}\alpha^{(l)}. \end{aligned} \tag{19.3}$$

当然, 利用 Farey 分割法可得到它的渐近公式, 现在我们要指出处理这一问题的另一途径.

设 $r_s(N_k,\cdots,N_1)$ 是下面的不定方程的解数:

$$\begin{cases} x_1^k+\cdots+x_s^k=N_k, \\ \qquad\cdots\cdots \\ x_1+\cdots+x_s=N_1, \end{cases} \quad 1\leqslant x_i\leqslant P. \tag{19.4}$$

当 $s>2t_0$($t_0$ 的定义见 §1) 时, 我们有

$$r_s(N_k,\cdots,N_1)=b_0P^{s-\frac12k(k+1)}\mathfrak{S}(N_k,\cdots,N_1)+O(P^{s-\frac12k(k+1)-c}), \tag{19.5}$$

这里

$$b_0=\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\Big(\int_0^1 e(\gamma_k x^k+\cdots+\gamma_1 x)\mathrm{d}x\Big)^s \times e\Big(-\frac{N_k}{P^k}\gamma_k-\cdots-\frac{N_1}{P}\gamma_1\Big)\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1, \tag{19.6}$$

$$\mathfrak{S}(N_k,\cdots,N_1)=\sum_{q_1,\cdots,q_k=1}^{\infty}A(q_k,\cdots,q_1), \tag{19.7}$$

$$A(q_k,\cdots,q_1)=\sum_{\substack{h_1=1\\(h_1,q_1)=1}}^{q_1}\cdots\sum_{\substack{h_k=1\\(h_k,q_k)=1}}^{q_k}S^s e\Big(-\frac{h_k}{q_k}N_k-\cdots-\frac{h_1}{q_1}N_1\Big),$$

以及

$$S=\frac{1}{Q}\sum_{x=1}^{O}e\Big(\frac{h_k}{q_k}x^k+\cdots+\frac{h_1}{q_1}x\Big),$$

其中 $Q$ 是 $q_k,\cdots,q_1$ 的最小公倍数.

这里将略去证明, 因为它和式 (1.3) 的证明完全相似. 虽然如此, 这里仍有一些关于收敛性的有趣问题, 因为本文中所遇到的是关于绝对收敛的问题. 式 (19.6) 和 (19.7) 中的收敛指数能大大减小. 例如, 式 (19.6) 当 $s\geqslant k$ 时收敛. 但作者在这里将不作仔细讨论.

当我们得到式 (19.5) 后, 就容易按照 Fourier 级数来具体处理 Proucht 问题和 Tarry 问题的情形. 事实上, 设

$$G(\alpha_k,\cdots,\alpha_1)=\Big(\sum_{x=1}^{P}e(\alpha_k x^k+\cdots+\alpha_1 x)\Big)^s.$$

式 (19.5) 就是断言函数 $G(\alpha_k,\cdots,\alpha_1)$ 的 Fourier 系数的性质. Tarry 问题等价于 Parseval 关系式:

$$\sum_{N_k}\cdots\sum_{N_1}r_s^2(N_k,\cdots,N_1)=\int_0^1\cdots\int_0^1|G(\alpha_k,\cdots,\alpha_1)|^2\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1.$$

Prouhet 问题就是要研究和式

$$r_s^{(l)}(P)=\sum_{N_k}\cdots\sum_{N_1}r_s^l(N_k,\cdots,N_1)$$

的性质.

若直接运用 Fourier 级数理论, 利用 Young-Hausdorff 定理就可得到

$$r_s^{(l)}(P)\leqslant\Big(\int_0^1\cdots\int_0^1|G(\alpha_k,\cdots,\alpha_1)|^{l/(l-1)}\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1\Big)^{l-1}$$

$$=O(P^{ls-\frac{1}{2}k(k+1)(l-1)}). \tag{19.8}$$

但是, 利用式 (19.5), 代替这个阶估计结果 (19.8), 就可得到 $r_s^{(l)}(P)$ 的渐近公式.

## 20. 注 记

1. 利用 Fourier 级数与殆周期函数之间的类似, 我们能处理下面的问题: 设

$$0 < e_1 < e_2 < \cdots < e_k$$

是 $k$ 个实数. 设 $r(N, \Delta)$ 是下述方程的整数解的个数:

$$\begin{aligned}
&|x_1^{e_1} + \cdots + x_s^{e_1} - N_1| \leqslant \Delta_1, \\
&\cdots\cdots \\
&|x_1^{e_k} + \cdots + x_s^{e_k} - N_k| \leqslant \Delta_k, \quad 1 \leqslant x_i \leqslant P,
\end{aligned}$$

其中 $\Delta_i$ 当 $P$ 趋于无穷时趋于零.

2. 利用文献 [1] 中的方法, 能得到 (1.1) 及 (19.4) 的解数的渐近公式, 即使限制我们的变数为素数, 且下界以 $t_0+1$ 代替 $t_0$ 也可以.

## 21. 在 $k=2$ 的情形, 我们的定理可达到最佳形式

**定理** 设 $r'(N)$ 是下述不定方程组的解数:

$$\begin{cases} x_1+x_2+x_3=y_1+y_2+y_3, & x_1^2+x_2^2+x_3^2 \leqslant N, \\ x_1^2+x_2^2+x_3^2=y_1^2+y_2^2+y_3^2, & y_1^2+y_2^2+y_3^2 \leqslant N. \end{cases} \tag{21.1}$$

那么, 当 $N \to \infty$ 时, 我们有

$$r'(N) \sim \frac{35\sqrt{3}}{2} N^{\frac{3}{2}} \log N. \tag{21.2}$$

**证明** 1) 设 $r(N_1, N_2)$ 是下述不定方程组的解数:

$$\begin{cases} x_1+x_2+x_3=N_1, \\ x_1^2+x_2^2+x_3^2=N_2, \quad N_2 \leqslant N. \end{cases} \tag{21.3}$$

那么, 利用 Schwartz 不等式可得

$$N_1^2 \leqslant 3N_2, \tag{21.4}$$

还有同余式

$$N_1 \equiv N_2 (\bmod 2). \tag{21.5}$$

从式 (21.3) 可得

$$x_1^2 + x_2^2 + (N_1 - x_1 - x_2)^2 = N_2,$$

即

$$(3x_1 - N_1)^2 + (3x_1 - N_1)(3x_2 - N_1)^2 + (3x_2 - N_1)^2 = \frac{3}{2}(3N_2 - N_1^2). \tag{21.6}$$

现来讨论下述不定方程的解数 $\Psi(m)$:

$$X_1^2 + X_1X_2 + X_2^2 = m, \tag{21.7}$$

我们知道

$$\psi(m) = 6\sum_{l|m}\left(\frac{-3}{l}\right). \tag{21.8}$$

若 $m$ 被 9 整除, 则从式 (21.7) 知 $(X_1, X_2)$, 因此, 当 $3|N_1$ 时, (21.6) 总可解, 且它的解数等于 $\psi\left(\frac{3}{2}(3N_2 - N_1^2)\right)$. 因此, 当 $3|N_1$ 时有

$$r(N_1, N_2) = \psi\left(\frac{3}{2}(3N_2 - N_1^2)\right). \tag{21.9}$$

若 $3 \nmid N_1$, 则有

$$\frac{3}{2}(3N_2 - N_1^2) \equiv 3 (\bmod 9).$$

从

$$X^2 + XY + Y^2 \equiv 3 (\bmod 9)$$

可得 $X \equiv Y \equiv \pm 1 (\bmod 3)$. 若 (21.7) 有解 $(X_1, X_2)$, 那么 $(-X_1, -X_2)$ 也有解. 所以

$$3x_1 - N_1 = \pm X_1, \quad 3x_2 - N_1 = \pm X_2$$

通过适当选取正负号也总是可解的, 且这种选取是唯一的. 所以当 $3 \nmid N_1$ 时,

$$r(N_1, N_2) = \frac{1}{2}\psi\left(\frac{3}{2}(3N_2 - N_1^2)\right). \tag{21.10}$$

因为

$$r'(N) = \sum_{N_1, N_2} r^2(N_1, N_2),$$

这里 $N_1$ 和 $N_2$ 遍历满足条件 (21.4) 和 (21.5) 的整数, 所以, 由式 (21.9) 及 (21.10) 得到

$$\begin{aligned} r'(N) =& \sum_{3|N_1}\sum_{N_2}\psi^2\left(\frac{3}{2}(3N_2-N_1^2)\right) \\ &+\frac{1}{4}\sum_{3\nmid N_1}\sum_{N_2}\psi^2\left(\frac{3}{2}(3N_2-N_1^2)\right) \\ =&S_1+\frac{1}{4}S_2, \end{aligned} \tag{21.11}$$

这里

$$S_1=\sum_{3|N_1}\sum_{N_2}\psi^2\left(\frac{3}{2}(3N_2-N_1^2)\right)$$

及

$$S_2=\sum_{3\nmid N_1}\sum_{N_2}\psi^2\left(\frac{3}{2}(3N_2-N_1^2)\right).$$

2) 因为 $\psi(m)=\psi(3m)$, 所以

$$S_2=\sum_{3\nmid N_1}\sum_{N_2}\psi^2\left(\frac{1}{2}(3N_2-N_1^2)\right), \tag{21.12}$$

这里 $m=\frac{1}{2}(3N_2-N_1^2)$, 使 $\frac{1}{2}(3N_2-N_1^2)$ 是平方数的项数等于方程

$$3N_2=N_1^2+2M^2,$$

的解数, 它是 $O(N_2^{\varepsilon})$. 因为 $\psi(N)=O(N^{\epsilon})$, 所以, 所有使 $\frac{1}{2}(3N_2-N_1^2)$ 为平方数的项数之和是

$$O\left(\sum_{N_2}O(N^{\varepsilon})\right)=O(N^{1+\varepsilon}). \tag{21.13}$$

以 $S_2^*$ 表示 $S_2$ 中 $\frac{1}{2}(3N_2-N_1^2)$ 不是一个平方数的那部分之和. 我们有

$$\begin{aligned} \psi(m) =&6\sum_{l|m}\left(\frac{-3}{l}\right) \\ =&6\sum_{\substack{l|m\\ l<\sqrt{m}}}\left(-\frac{3}{l}\right)+6\sum_{\substack{l|m\\ l<\sqrt{m}}}\left(\frac{-3}{m/l}\right) \\ =&6\left(1+\left(\frac{-3}{m}\right)\right)\sum_{\substack{l|m\\ l<\sqrt{m}}}\left(\frac{-3}{l}\right). \end{aligned}$$

因为, 当 $m=\frac{1}{2}(3N_2-N_1^2)$ 时,

$$\left(\frac{-3}{m}\right)=\left(\frac{-3}{N_2^2}\right)=1,$$

故有

$$\begin{aligned}S_2^* =&144\sum_{3\nmid N_1}\sum_{N_2}\Bigg(\sum_{\substack{l\mid m\\ l<\sqrt{m}}}\left(\frac{-3}{l}\right)\Bigg)^2\\ =&144\sum_{l<\sqrt{\frac{3N}{2}}}\sum_{l'<\sqrt{\frac{3N}{2}}}\left(\frac{-3}{ll'}\right)\Lambda(l,l'),\end{aligned} \tag{21.14}$$

这里 $\Lambda(l,l')$ 是

$$\frac{1}{2}(3N_2-N_1^2)\equiv 0\left(\bmod\frac{ll'}{(l,l')}\right),\quad N_1^2\leqslant 3N_2\leqslant 3N$$

的解数. 因此有

$$\begin{aligned}\Lambda(l,l')=&\sum_{N_1}\left(\frac{N-N_1^2/3}{2ll'/(l,l')}+O(1)\right)\\ =&\sum_{N_1^2\leqslant 3N}\frac{(N-N_1^2/3)(l,l')}{2ll'}+O(N^{\frac{1}{2}}),\\ =&\frac{(l,l')}{2ll'}\frac{5}{\sqrt{3}}N^{\frac{3}{2}}+O\left(\frac{(l,l')}{ll'}N\right)+O(N^{\frac{1}{2}}),\end{aligned} \tag{21.15}$$

因为

$$\sum_{N_1^2\leqslant 3N}N=N(2[\sqrt{3N}]+1)=2\sqrt{3}N^{\frac{3}{2}}+O(N)$$

及

$$\sum_{N_1^3\leqslant 3N}\frac{N_1^2}{3}=\frac{1}{9}(\sqrt{3N})^3+O(N).$$

由式 (21.14) 及 (21.15), 就得到

$$\begin{aligned}S_2^* =&120\sqrt{3}N^{\frac{3}{2}}\sum_{l<\sqrt{\frac{3N}{2}}}\sum_{l'<\sqrt{\frac{3N}{2}}}\frac{(l,l')}{ll'}\left(\frac{-3}{ll'}\right)\\ &+O\left(N\sum_{l<\sqrt{\frac{3N}{2}}}\sum_{l'<\sqrt{\frac{3N}{2}}}\frac{(l,l')}{ll'}\right)+O(N^{\frac{3}{2}})\end{aligned}$$

$$=120\sqrt{3}N^{\frac{3}{2}}\sum_{l<\sqrt{\frac{3N}{2}}}\sum_{l'<\sqrt{\frac{3N}{2}}}\frac{(l,l')}{ll'}\left(\frac{-3}{ll'}\right)+O(N^{\frac{3}{2}}),\tag{21.16}$$

因为 $(l,l')\leqslant\sqrt{ll'}$,

$$\sum_{l<\sqrt{\frac{3N}{2}}}\sum_{l'<\sqrt{\frac{3N}{2}}}\frac{(l,l')}{ll'}\leqslant\left(\sum_{l<\sqrt{\frac{3N}{2}}}\frac{1}{l^{1/2}}\right)^2=O(N^{\frac{1}{2}}).$$

3) 现在来证明

$$\sum_{l<\sqrt{\frac{3N}{2}}}\sum_{l'<\sqrt{\frac{3N}{2}}}\frac{(l,l')}{ll'}\left(\frac{-3}{ll'}\right)=\frac{1}{12}\log N+O((\log N)^{\frac{1}{2}}).\tag{21.17}$$

证明中将用到以下事实:

$$\sum_{a\leqslant m\leqslant b}\frac{1}{m}\left(\frac{-3}{m}\right)=O\left(\frac{1}{a}\right),\tag{21.18}$$

这是分部求和及熟知的结果

$$L_{-3}(1)=\sum_{m=1}^{\infty}\frac{1}{m}\left(\frac{-3}{m}\right)=\frac{\pi}{3\sqrt{3}}\tag{21.19}$$

的一个推论.

设 $l=md,l'=m'd$ 及 $(m,m')=1$. 首先考虑式 (21.17) 中由 $d>\sqrt{N}/\log N$ 那些项组成的部分和. 它不超过

$$\begin{aligned}&\sum_{\frac{\sqrt{N}}{\log N}<d<\sqrt{\frac{3N}{2}}}\sum_{\substack{m<\sqrt{\frac{3N}{2}}\frac{1}{d}\ m'<\sqrt{\frac{3N}{2}}\frac{1}{d}\\(m,m')=1}}\frac{1}{dmm'}\\ \leqslant&\sum_{\frac{\sqrt{N}}{\log N}<d<\sqrt{\frac{3N}{2}}}\frac{1}{d}\sum_{m<\sqrt{\frac{3}{2}}\log N}\frac{1}{m}\sum_{m'<\sqrt{\frac{3}{2}}\log N}\frac{1}{m'}\\ =&O((\log\ \log N)^3).\end{aligned}\tag{21.20}$$

和式 (21.17) 中余下的那部分等于

$$\begin{aligned}U=&\sum_{\substack{d<\sqrt{N}/\log N\\3\nmid d}}\sum_{\substack{m<\sqrt{\frac{3N}{2}}\frac{1}{d}\ m'<\sqrt{\frac{3N}{2}}\frac{1}{d}\\(m,m')=1}}\frac{1}{dmm'}\left(\frac{-3}{mm'}\right)\\ =&\sum_{\substack{d<\sqrt{N}/\log N\\3\nmid d}}\sum_{m<\sqrt{\frac{3N}{2}}\frac{1}{d}}\sum_{m'<\sqrt{\frac{3N}{2}}\frac{1}{d}}\frac{1}{dmm'}\left(\frac{-3}{mm'}\right)\sum_{m|(m,m')}\mu(n).\end{aligned}\tag{21.21}$$

设 $m=nq, m'=nq'$, 我们有

$$U=\sum_{\substack{d<\sqrt{N}/\log N\\ 3\nmid d}}\frac{1}{d}\sum_{\substack{n<\sqrt{\frac{3N}{2}\frac{1}{d}}\\ 3\nmid n}}\frac{\mu(n)}{n^2}\sum_{q<\sqrt{\frac{3N}{2}}\frac{1}{dn}}\sum_{q'<\sqrt{\frac{3N}{2}}\frac{1}{dn}}\frac{1}{qq'}\left(\frac{-3}{qq'}\right)$$

$$=U_1+U_2, \tag{21.22}$$

其中 $U_1$ 是由那些 $n>\left(\sqrt{\frac{3N}{2}\frac{1}{d}}\right)^{\frac{1}{2}}$ 的项组成的和, 而 $U_2$ 是 $U$ 的余下部分. 这样, 由式得到

$$U_1\leqslant\sum_{d<\sqrt{N}/\log N}\frac{1}{d}\sum_{(\sqrt{\frac{3N}{2}\frac{1}{d}})^{\frac{1}{2}}<n}\frac{1}{n^2}\left|\sum_{q<\sqrt{\frac{3N}{2}}\frac{1}{dn}}\frac{1}{q}\left(\frac{-3}{q}\right)\right|\times\left|\sum_{q'<\sqrt{\frac{3N}{2}}\frac{1}{dn}}\frac{1}{q'}\left(\frac{-3}{q'}\right)\right|$$

$$=O\left(\log N\sum_{(\log N)^{\frac{1}{2}}<n}\frac{1}{n^2}\right)=O((\log N)^{\frac{1}{2}}). \tag{21.23}$$

现来讨论

$$U_2=\sum_{\substack{d<\sqrt{N}/\log N\\ 3\nmid d}}\frac{1}{d}\sum_{\substack{n<(\sqrt{\frac{3N}{2}\frac{1}{d}})^{\frac{1}{2}}\\ 3\nmid n}}\frac{\mu(n)}{n^2}\left(\sum_{q<\sqrt{\frac{3N}{2}}\frac{1}{dn}}\frac{1}{q}\left(\frac{-3}{q}\right)\right)^2.$$

因为当 $d<\sqrt{N}/\log N$ 时,

$$\sum_{n>(\sqrt{\frac{3N}{2}\frac{1}{d}})^{\frac{1}{2}}}\frac{\mu(n)}{n^2}=O\left(\left(\sqrt{\frac{3N}{2}\frac{1}{d}}\right)^{-\frac{1}{2}}\right)=O\left((\log N)^{-\frac{1}{2}}\right)$$

以及由式 (21.19) 知

$$\sum_{q<\sqrt{\frac{3N}{2}}\frac{1}{dn}}\left(\frac{-3}{q}\right)\frac{1}{q}=O\left(\left(\sqrt{\frac{3N}{2}}\frac{1}{dn}\right)^{-1}\right)=O\left((\log N)^{-\frac{1}{2}}\right),$$

所以有

$$U_2=\sum_{\substack{d<\sqrt{N}/\log N\\ 3\nmid d}}\frac{1}{d}\sum_{\substack{n=1\\ 3\nmid n}}^{\infty}\frac{\mu(n)}{n^2}L_{-3}^2(1)+O\left((\log N)^{\frac{1}{2}}\right)$$

$$=\frac{9}{4\pi^2}\log N L_{-3}^2(1)+O\left((\log N)^{\frac{1}{2}}\right), \tag{21.24}$$

这里用到了

$$\sum_{\substack{d<\sqrt{N}/\log N\\ 3\nmid d}}\frac{1}{d}=\sum_{d<\sqrt{N}/\log N}\frac{1}{d}-\frac{1}{3}\sum_{d<\frac{1}{3}\sqrt{N}/\log N}\frac{1}{d}$$

$$=\frac{1}{3}\log N+O(\log\log N),$$

$$\sum_{\substack{n=1\\3\nmid n}}^{\infty}\frac{\mu(n)}{n^2}=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}-\frac{1}{9}\sum_{\substack{m=1\\3\nmid m}}^{\infty}\frac{\mu(3m)}{m^2}=\frac{1}{\zeta(2)}+\frac{1}{9}\sum_{\substack{m=1\\3\nmid m}}^{\infty}\frac{\mu(m)}{m^2},$$

以及

$$\sum_{\substack{n=1\\3\nmid n}}^{\infty}\frac{\mu(n)}{n^2}=\frac{9}{8}\frac{1}{\zeta(2)}=\frac{27}{4\pi^2}.$$

综合式 (21.20), (21.21), (21.22), (21.23) 及 (21.24), 就推得式 (21.17). 进而, 由式 (21.16) 及 (21.17), 就得到

$$S_2=10\sqrt{3}N^{\frac{3}{2}}\log N+O(N^{\frac{3}{2}}(\log N)^{\frac{1}{2}}).$$

4) 现在来求 $S_1$ 的渐近公式. 设 $\tau$ 是整除 $\frac{3}{2}(3N_2-N_1^2)$ 的 3 的最高方幂, 这里 $\tau\geqslant 2$. 我们按 $\tau$ 来对 $S_1$ 求和. 这样就有

$$S_1=\sum_{\tau=2}^{W}\sum_{\substack{N_1\quad N_2\\3^\tau\|\frac{3}{2}(3N_2-N_1^2)}}\sum\psi^2\left(\frac{3}{2}(3N_2-N_1^2)\right),$$

这里

$$W=\left[\log\frac{9}{2}N/\log 3\right].$$

因为 $\psi(3N)=\psi(N)$, 故有

$$S_1=\sum_{\tau=1}^{W}\sum_{N_1}\sum_{N_2}\psi^2(m),$$

其中 $m=\frac{3}{2}(3N_2-N_1^2)3^{-\tau}$. 我们来讨论和式

$$S'_1=\sum_{\tau\geqslant W/2}\sum_{N_1}\sum_{N_2}\psi^2(m),$$

它是

$$O\Big(N^{\varepsilon}\sum_{\tau\geqslant W/2}\sum_{N_1}\sum_{N_2}1\Big),$$

以及

$$\frac{3}{2}(3N_2-N_1^2)\equiv 0(\bmod 3^\tau),\quad N_1^2\leqslant 3N_2\leqslant 3N$$

的解数是

$$O\left(\sum_{N_1}\left(\frac{N-\frac{1}{3}N_1^2}{3^\tau}+1\right)\right)=O\left(\left(\frac{N^{3/2}}{3^\tau}+1\right)\right).$$

因而有

$$S'_1=O\left(N^\varepsilon\sum_{\tau\geqslant\frac{1}{2}W}\left(\frac{M^{3/2}}{3^\tau}+1\right)\right)=O(N^{\frac{3}{2}+\varepsilon}/3^{\frac{1}{2}W})=O(N^{1+\varepsilon}).$$

如同处理 $S_2$ 一样, 我们能证明 $S_1$ 中由 $m$ 是一平方数 ($\geqslant 0$) 的那些项组成的部分和 $S_1''$ 也是一个低阶量.

现在我们来考虑

$$S_1-S'_1+S''_1=\sum_{\tau\leqslant\frac{1}{2}W}\sum_{N_1}\sum_{N_2}\psi^2(m)=S_1''',$$

因为 $m$ 不是平方数, 故有

$$\begin{aligned}\psi(m)&=6\sum_{\substack{l<\sqrt{m}\\ l\mid m}}\left(\frac{-3}{l}\right)+6\sum_{l<\sqrt{m}}\left(\frac{-3}{m/l}\right)\\&=6\left(1+\left(\frac{-3}{m}\right)\right)\sum_{l<\sqrt{m}}\left(\frac{-3}{l}\right)\\&=\begin{cases}0, & m\equiv 2(\bmod 3),\\ 12\sum\limits_{l<\sqrt{m}}\left(\frac{-3}{l}\right), & m\equiv 1(\bmod 3).\end{cases}\end{aligned}$$

所以有

$$\begin{aligned}S_1'''&=144\sum_{\tau=1}^{W/2}\sum_{\substack{N_1\\ m\equiv 1(3)}}\sum_{N_2}\left(\sum_{l<\sqrt{m}}\left(\frac{-3}{l}\right)\right)^2\\&=144\sum_{\tau=2}^{W/2}\sum_{l<\sqrt{m}}\sum_{l'<\sqrt{m}}\left(\frac{-3}{l}\right)\left(\frac{-3}{l'}\right)\Lambda(l,l';\tau),\end{aligned}$$

这里 $\Lambda(l,l';\tau)$ 是

$$\frac{1}{2}(3N_2-N_1^2)\equiv 0\quad\left(\bmod 3^{\tau-1}\frac{ll'}{(l,l')}\right),\quad N_1^2\leqslant 3N_2\leqslant 3N$$

的解数. 因而有

$$\Lambda(l,l';\tau)=\sum_{N_1^2\leqslant 3N}\left(\frac{\left(N-\frac{1}{3}N_1^2\right)(l,l')}{2\cdot 3^{\tau-2}ll'}+O(1)\right)$$

$$=\frac{(l,l')}{2ll'}\frac{5}{\sqrt{3}}\frac{1}{3^{\tau-2}}N^{\frac{3}{2}}+O\left(\frac{(l,l')}{3^{\tau}ll'}N\right)+O(N^{\frac{1}{2}}).$$

类似于 3), 我们有

$$S_1=120\sqrt{3}N^{\frac{3}{2}}\sum_{\tau=2}^{W/2}\sum_{l\leqslant\sqrt{\frac{3N}{2\cdot 3^{\tau}}}}\sum_{l'\leqslant\sqrt{\frac{3N}{2\cdot 3^{\tau}}}}\frac{(l,l')}{ll'}\left(\frac{-3}{ll'}\right)\frac{1}{3^{\tau-2}}+O(N^{\frac{3}{2}})$$

$$=120\sqrt{3}\frac{3}{2}N^{\frac{3}{2}}\frac{\log N}{12}+O(N^{\frac{3}{2}}(\log N^{\frac{1}{2}})).$$

综合关于 $S_1$ 和 $S_2$ 的两个估计, 我们就得到

$$r'(N)=10\sqrt{3}\left(\frac{3}{2}+\frac{1}{4}\right)N^{\frac{3}{2}}\log N+O(N^{\frac{3}{2}}(\log N)^{\frac{1}{2}})$$

$$=\frac{35\sqrt{3}}{2}N^{\frac{3}{2}}\log N+O(N^{\frac{3}{2}}(\log N)^{\frac{1}{2}}).$$

求 (21.1) 的解数的另一可能途径是考虑不定五元二次型

$$x_1^2+x_2^2+x_3^2-y_1^2-y_2^2-(x_1+x_2+x_3-y_1-y_2)^2.$$

但是, 看起来为了去建立本原解的条件与 (21.1) 形式的条件之间的联系将是更为复杂.

## 参 考 文 献

[1] Hua, Loo-Keng(华罗庚). Аддитивная теория простых чисед, труды математического института Стеклова, X X II, 1947.

[2] Hua, Loo-Keng(华罗庚). An improvement of Vinogradov's mean-value theorem and several applications. *Quart. Journ. of Math.* (Oxford), 1949, 20: 48–61.

[3] Hua, Loo-Keng(华罗庚). On Tarry's problem. *ibid.* (Oxford), 1928, 9: 315–320.

[4] Hua, Loo-Keng(华罗庚). On an exponential sum. *Journ. Chinese. Math. Soc.*, 1939, 2.

[5] Виноградов И М. Метод тригонометрических сумм в теории чисед. Труды математического института Стеклова, X XIII, 1947.

[6] Hua, Loo-Keng(华罗庚). Математ. сборник,1938, 3: 435–471.

[7] Mordell. Quart. *Journ. of Math.*, 1939, 3: 161–167.

(潘承彪 译)

# 关于指数和①

华罗庚 (中国科学院数学研究所)

这篇短文的目的是证明下面的定理, 但它的推广与应用则不在这里讨论.

**定理** 设整数 $k \geqslant 2$, 及 $(h,q)=1$. 那么, 对任意的 $\varepsilon>0$ 有

$$\sum_{x=1}^{P} \mathrm{e}^{2\pi \mathrm{i} h x^k/q} = \frac{P}{q}\sum_{x=1}^{q} \mathrm{e}^{2\pi \mathrm{i} h x^k/q} + O(q^{\frac{1}{2}+\varepsilon}),$$

这里符号 $O$ 所包含的常数仅和 $k$ 及 $\varepsilon$ 有关.

这定理改进了作者[1] 1940 年的一个结果. 在更广的范围内, 改进了 Vinogradov[2] 的一个著名结果.

定理的证明是基于下面的几个引理.

**引理 1**[3,4] 设 $p$ 是素数, 及

$$f(x)=a_kx^k+\cdots+a_1x+a_0, \quad p \nmid (a_k,\cdots,a_1).$$

我们有

$$\left|\sum_{x=1}^{P} \mathrm{e}^{2\pi \mathrm{i} f(x)/p}\right| \leqslant k\sqrt{p}. \tag{1}$$

**引理 2** 在引理 1 的假设下, 再假定 $p^t|(ka_k,\cdots,2a_2,a_1)$, 及同余方程

$$p^{-t}f(x)\equiv 0 \pmod p, \quad 0\leqslant x<p \tag{2}$$

没有重根, 那么有

$$\left|\sum_{x=1}^{p^l} \mathrm{e}^{2\pi \mathrm{i} f(x)/p^l}\right| \leqslant k^{\frac{5}{2}}p^{\frac{l}{2}}. \tag{3}$$

**证明** 设 $\mu_1,\cdots,\mu_r (r\leqslant k-1)$ 是 (2) 的根. 因为 $p^t<k$, 所以引理显然是下述不等式的一个推论:

$$\left|\sum_{x=1}^{p^l} \mathrm{e}^{2\pi \mathrm{i} f(x)/p^l}\right| \leqslant k\max(1,r)p^{\frac{1}{2}(l+t)}. \tag{4}$$

---

① 1956 年 11 月 29 日收到. 发表于 *Sci. Record* (*N. S*), 1957, 1: 1-4.

1) 当 $l < 2(t+1)$ 时, 若 $t=0$, 则 $l=1$, 式 (4) 由引理 1 推出; 若 $t \geqslant 1$, 则有

$$\left|\sum_{x=1}^{p^l} \mathrm{e}^{2\pi \mathrm{i} f(x)/p^l}\right| \leqslant p^l \leqslant p^{\frac{1}{2}(l+t)} p^{\frac{1}{2}(l-t)} \leqslant p^{\frac{1}{2}(l+1)} p^{\frac{1}{2}(l+t)} \leqslant k p^{\frac{1}{2}(l+t)}.$$

2) 当 $l \geqslant 2(t+1)$ 时, 我们有

$$\left|\sum_{x=1}^{p^l} \mathrm{e}^{2\pi \mathrm{i} f(x)/p^l}\right| \leqslant \sum_{j=1}^{r} \left|\sum_{y=1}^{p^{l-1}} \mathrm{e}^{2\pi \mathrm{i}(f(\mu_j+py)-f(\mu_j))/p^l}\right|. \tag{5}$$

注意到在这情形, (2) 无解, 即 $r=0$, 所以式 (5) 两边均为零.

现设 $g_j(x) = p^{-\sigma_j}(f(\mu_j+px)-f(\mu_j)), j=1,\cdots,r$, 这里 $p$ 不能整除 $g_j(x)$ 的所有系数. 因为 $f(\mu_j) \not\equiv 0(\mathrm{mod} p^{t+1})(j=1,\cdots,r)$, 所以有 $2 \leqslant \sigma_j \leqslant t+2$, 以及由 (5) 得

$$\left|\sum_{x=1}^{p^l} \mathrm{e}^{2\pi \mathrm{i} f(x)/p^l}\right| \leqslant \begin{cases} r p^{l-1} \leqslant r p^{t+1} \leqslant rkp, & l \leqslant \max(\sigma_1,\cdots,\sigma_r), \\ \displaystyle\sum_{j=1}^{r} p^{\sigma_j-1} \left|\sum_{x=1}^{p^{l-\sigma_j}} \mathrm{e}^{2\pi \mathrm{i} g_j(x)/p^{l-\sigma_j}}\right|, & l > \max(\sigma_1,\cdots,\sigma_r). \end{cases} \tag{6}$$

对后一情形用归纳法, 设 $p^{\delta_j}$ 整除 ${g'}_j(x)$ 的所有系数, 但 $p^{\delta_j+1}$ 不能. 从表达式

$$p^{\sigma_j} g_j'(x) = f'(\mu_j)p + f''(\mu_j)p^2 x + \cdots + \frac{f^{(k)}(\mu_j)}{(k-1)!} p^k x^{k-1}$$

可以看出 $\sigma_j + \delta_j = t+2$. 同余方程

$$p^{-\delta_j} g_j'(x) \equiv f'(\mu_j)p^{-t-1} + f''(\mu_j)p^{-t} x \equiv 0(\mathrm{mod} p), \quad 0 \leqslant x < p$$

仅有一个解, 故由归纳法得

$$\left|\sum_{x=1}^{p^l} \mathrm{e}^{2\pi \mathrm{i} f(x)/p^l}\right| \leqslant \sum_{j=1}^{r} p^{\sigma_j-1} k p^{\frac{1}{2}(l-\delta_j+\sigma_j)} = krp^{\frac{1}{2}(l+t)}.$$

引理证毕.

**引理 3** 设 $\sigma \geqslant 0$ 及 $S(p^l,p^\sigma) = \max\limits_{p \nmid hm} \left|\sum_{x=1}^{p^l} \mathrm{e}^{2\pi \mathrm{i}(hx^k+p^\sigma mx)/p^l}\right|$, 那么有

$$S(p^l,p^\sigma) \leqslant k^{\frac{5}{2}} p^{\frac{1}{2}(l+\sigma)}.$$

**证明** 当 $l=1$ 时, 由引理推出结论成立.

现假定 $l \geqslant 2, k = p^{\theta}k_1, p \nmid k_1$.

设 $\theta \geqslant \sigma$. 若同余方程

$$f'(x) = p^{\theta}k_1hx^{k-1} + p^{\sigma}m \equiv 0 \pmod{p^{\sigma+1}}, \quad 0 \leqslant x < p$$

无解或有 $(k-1, p-1)$ 个单根, 那么由引理 2 推出

$$\left|\sum_{x=1}^{p^l} \mathrm{e}^{2\pi\mathrm{i}(hx^k+p^{\sigma}mx)/p^l}\right| \leqslant k^{\frac{5}{2}}p^{\frac{l}{2}}.$$

若不然, 则 $p|k-1, \theta = \sigma = 0$, 用类似的但更精细的方法可得同样的结论.

假如 $\theta < \sigma$. 当 $l < 2(\theta+1)$ 时, 显有 $S(p^l, p^{\tau}) \leqslant k^{\frac{5}{2}}p^{\frac{l}{2}}$. 当 $l \geqslant 2(\theta+1)$ 时, 同余方程 $k_1hx^{k-1} + p^{\sigma-\theta}m \equiv 0 \pmod p, 0 \leqslant x < p$ 仅有单根 $x = 0$. 因而有

$$\begin{aligned}\left|\sum_{x=1}^{p^l} \mathrm{e}^{2\pi\mathrm{i}(hx^k+p^{\sigma}mx)/p^l}\right| &\leqslant \left|\sum_{x=1}^{p^{l-1}} \mathrm{e}^{2\pi\mathrm{i}(hp^kx^k+p^{\sigma+1}mx_1)/p^l}\right| \\ &\leqslant p^{k-1}\left|\sum_{x=1}^{p^{l-k}} \mathrm{e}^{2\pi\mathrm{i}(hx^k+p^{\sigma+1-k}mx_1)/p^{l-k}}\right|, \quad l > k, \sigma+1 \geqslant k, \\ &= \begin{cases} 0, & l > k, \sigma+1 < k, \\ 0, & l \leqslant k, \sigma+1 < l, \\ p^{l-1} \leqslant p^{\frac{1}{2}(l+\sigma-1)}, & l \leqslant k, \sigma+1 \geqslant l. \end{cases}\end{aligned}$$

在后三种情形, 引理显然成立, 而对第一种情形, 用归纳法可得

$$\left|\sum_{x=1}^{p^l} \mathrm{e}^{2\pi\mathrm{i}(hx^k+p^{\sigma}mx)/p^l}\right| \leqslant p^{k-1}k^{\frac{5}{2}}p^{\frac{1}{2}(l-k+\sigma+1-k)} \leqslant k^{\frac{5}{2}}p^{\frac{1}{2}(l-\sigma)}.$$

引理证毕.

**定理的证明**　显然可假定 $1 \leqslant P \leqslant q$, 这时有

$$\begin{aligned}\sum_{x=1}^{P} \mathrm{e}^{2\pi\mathrm{i}hx^k/q} &= \frac{1}{q}\sum_{n=1}^{q}\sum_{x=1}^{q} \mathrm{e}^{2\pi\mathrm{i}(hx^k+nx)/q}\sum_{t=1}^{P} \mathrm{e}^{-2\pi\mathrm{i}nt/q} \\ &= \frac{P}{q}\sum_{x=1}^{q} \mathrm{e}^{2\pi\mathrm{i}hx^k/q} + O\left(\frac{1}{q}\sum_{n=1}^{q-1}\left|\sum_{t=1}^{P} \mathrm{e}^{2\pi\mathrm{i}nt/q}\right| \cdot \left|\sum_{x=1}^{q} \mathrm{e}^{2\pi\mathrm{i}(hx^k+nx)/q}\right|\right) \\ &= \frac{P}{q}\sum_{x=1}^{q} \mathrm{e}^{2\pi\mathrm{i}hx^k/q} + O\left(\sum_{n=1}^{q-1}\frac{1}{n}\left|\sum_{x=1}^{q} \mathrm{e}^{2\pi\mathrm{i}(hx^k+nx)/q}\right|\right)\end{aligned}$$

设 $q=p_1^{l_1}\cdots p_s^{l_s}$ 是 $q$ 的标准分解式, 现考虑 $\sum_{n=1}^{q-1}\frac{1}{n}\left|\sum_{x=1}^{q}\mathrm{e}^{2\pi\mathrm{i}(hx^k+nx)/q}\right|$ 中满足条件 $p_1^{a_1}\cdots p_s^{a_s}|n$ 但 $p_1^{a_1+1}\nmid n,\cdots,p_s^{a_s+1}\nmid n$ 的项之和. 若能证明这些项之和是 $O\left(\frac{q^{\frac{1}{2}+\varepsilon}}{(p_1^{a_1}\cdots p_s^{a_s})^{\frac{1}{2}}}\right)$, 那么就证明了定理. 设 $n=p_1^{a_1}\cdots p_s^{a_s}m,(m,p_1\cdots p_s)=1$. 这部分和

$$\begin{aligned}&\leqslant\sum_{\substack{m\geqslant q-1\\(m,q)=1}}\frac{1}{p_1^{a_1}\cdots p_s^{a_s}m}\prod_{i=1}^{s}S(p_i^{l_i},p_i^{a_i})\\&\leqslant R^{\frac{5}{2}s}\frac{p_1^{\frac{1}{2}(l_1+a_1)}\cdots p_s^{\frac{1}{2}(l_s+a_s)}}{p_1^{a_1}\cdots p_s^{a_s}}\log q=O\left(\frac{q^{\frac{1}{2}+\varepsilon}}{(p_1^{a_1}\cdots p_s^{a_s})^{\frac{1}{2}}}\right).\end{aligned}$$

因而定理得证.

## 参考文献


[1] Hua L K (华罗庚). On an exponential sum. *Journ. of Chinese Math. Soc.*, 1940, 2: 301–312; *Additive Prime Number Theory.* Acad. Sinica Press, 1953: 11–12.

[2] Биноградов И м. Избранные Труды, Иэдателъство Акад. Наук СССР, Москва, 1952: 291–295.

[3] Weil A. On the Riemann hypothesis in functional fields. *Proc. of Nat. Acad. of Sci. of U. S. A.*, 1941, 27: 345–347.

[4] Carlitz l and Uchiyama S. Bounds for Exponential Sums (in print).


(潘承彪 译)

# 关于华林问题的优弧①

华罗庚 (中国科学院, 数学研究所)

设 $k$ 是一个 $\geqslant 3$ 的整数, $N$ 为整数及 $P$ 为 $N^{\frac{1}{k}}$ 的整数部分. 设

$$T(\alpha)=\sum_{x=1}^{P}\mathrm{e}^{2\pi\mathrm{i}x^k\alpha}.$$

于是

$$r(N)=\int_0^1 T^s(\alpha)\mathrm{e}^{-2\pi\mathrm{i}N\alpha}\mathrm{d}\alpha$$

等于方程

$$x_1^k+\cdots+x_s^k=N,\quad 1\leqslant x_\nu\leqslant P$$

的整数解的个数.

华林问题研究的最重要的问题之一, 是要对于最小的 $s$, 找到当 $N\to\infty$ 时以上解数的渐近公式. 由于周期性, 我们可将区间 (0,1) 代之以 $\left(-\frac{1}{r},1-\frac{1}{r}\right)$, 其中 $r=P^{k-1+\varepsilon}$, 而 $\varepsilon>0$ 为任意给定的小常数. 我们考虑子区间 $\mathfrak{M}_{h,q}$,其中心在有理点 $\frac{h}{q}$, 长度为 $\frac{2}{qr}$, 这里 $(h,q)=1, 1\leqslant h\leqslant q\leqslant P^{1-\varepsilon}$. 这些子区间没有公共点. 区间的剩余部分记做 $E$. 按照传统, $\mathfrak{M}_{h,q}$ 称为优弧. 通常 $r(N)$ 的主阶来自于优弧上的积分, 即

$$I=\sum_{h,q}\int_{\mathfrak{M}_{h,q}}T^s(\alpha)\mathrm{e}^{-2\pi\mathrm{i}N\alpha}\mathrm{d}\alpha\sim\mathfrak{S}(N)\frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)}N^{\frac{s}{k}-1},\tag{1}$$

这里 $\mathfrak{S}(N)$ 表示奇异级数.

自从 Hardy 和 Littlewood 发明圆法以来, 除去他们证明了当 $s\geqslant 2k+1$ 时 (1) 式成立之外, 相应的进展甚少. 本文的目的是要宣布, 我们可以对于 $s\geqslant k+1$ 证明 (1) 式. 从某种意义上讲, 这是最佳可能的结果. 它的证明主要用到了著名的 Euler 求和公式和作者[1] 关于三角和的新估计. 更明确地, 我们是证明了下面的渐近公式:

---

① 1957 年 4 月 1 日收到. 发表于*Sci. Record, new series*, 1957, 1(3): 17–18.

在 $\mathfrak{M}_{h,q}$ 上, 有

$$T(\alpha)=\frac{1}{q}\sum_{x=1}^{q}\mathrm{e}^{2\pi\mathrm{i}\frac{h}{q}x^k}\int_0^P \mathrm{e}^{2\pi\mathrm{i}\beta y^k}\mathrm{d}y+O(q^{\frac{1}{2}+\varepsilon}).$$

再由一系列的引理, 就可以得到所宣布的结果.

此外, 作者的方法也可以用于处理集合 $E$ 中的一部分. 例如, 我们可以知道, 来自于有理点 $\frac{h}{q}(P^{1-\varepsilon}\leqslant q\leqslant P^{1-\frac{1}{2k}})$ 的邻域中的贡献, 其阶要低于 (1) 式中的阶.

## 参 考 文 献

[1] Hua L K. On exponential sums. *Sci. Record*, 1957, 1(1): 1–4.

(潘承彪 译)

# 《华罗庚文集》已出版书目

（按出版时间排序）

1 华罗庚文集数论卷 I 王元 审校 2010 年 5 月
2 华罗庚文集数论卷 II 贾朝华 审校 2010 年 5 月
3 华罗庚文集数论卷 III 王元 潘承彪 贾朝华 编译 2010 年 5 月
4 华罗庚文集代数卷 I 万哲先 审校 2010 年 5 月
5 华罗庚文集多复变函数论卷 I 陆启铿 审校 2010 年 5 月
6 华罗庚文集应用数学卷 I 杨德庄 主编 2010 年 5 月
7 华罗庚文集应用数学卷 I 杨德庄 主编 2010 年 5 月
8 华罗庚文集代数卷 II 待定
9 华罗庚文集多复变函数论卷 II 待定